Council of the European Union

Brussels, 6 March 2026
(OR. en)

6033/26
ADD 1

SOC 55
GENDER 11
ANTIDISCRIM 10
JAI 160
DROIPEN 22
TELECOM 53
CYBER 48
JEUN 19

NOTE

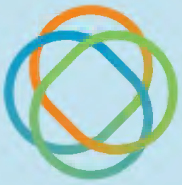
From:	General Secretariat of the Council
To:	Delegations
Subject:	From lived reality to policy action: Combating cyber violence against girls in the EU - *EIGE report*

Delegations will find attached the report entitled "From lived reality to policy action: Combating cyber violence against girls in the EU" prepared by the European Institute for Gender Equality (EIGE).

European Institute for Gender Equality

From lived reality to policy action: Combatting cyber violence against girls in the EU

An EU Agency



European Institute for
Gender Equality

European Institute for Gender Equality

EIGE Gedimino pr. 16

LT-01103 Vilnius

LITHUANIA

Tel. +370 52157444

Contributors

IRS – Istituto per la ricerca sociale and Mediterranean Institute of Gender Studies (MIGS) provided the study on which this report is based.

Dr. Leonie Tanczer provided inputs to an early draft.

Sincere thanks are due to the participants of EIGE's consultation meeting held remotely on November 12th, 2025 for their feedback on draft policy recommendations.

The participants included: Elizabeth Ávila González, Kim Barker, Stephanie Futter-Orel, Inès Girard, Olga Jurasz, Zuzanna Kowalska (FRA), Marlene Matos, Janine Mc Ginn, Eva O'Byrne, Adèle Philtjens, Lisa Robinson, Silvia Semenzin, Sara Sighinolfi (FRA), Sylwia Spurek and Leonie Tanczer.

Abbreviations

AI	Artificial Intelligence
APAV	Portuguese Association for Victim Support
BIK	Better Internet for Kids
BPfA	Beijing Platform for Action
CBS	Dutch Central Bureau of Statistics
CoE	Council of Europe
CSA	*Conseil supérieur de l'audiovisuel*
CSAM	Child sexual abuse material
CVAWG	Cyber violence against women and girls
DM	Direct messaging
DSA	Digital Services Act
EU	European Union
ENISA	The European Union Agency for Cybersecurity
EWL	European Women's Lobby
FEMM	Committee on Women's Rights and Gender Equality
FRA	European Union Agency for Fundamental Rights
GBV	Gender-based violence
GDPR	General Data Protection Regulation
GREVIO	Group of Experts on Action against Violence against Women and Domestic Violence
HBSC	Health Behaviour in School-aged Children

HUDOC	European Court of Human Rights
ICT	Information and communication technologies
LIBE	Committee on Civil Liberties, Justice and Home Affairs
MS	Member States
NGO	Non-governmental organisation
UN	United Nations
VAWG	Violence against women and girls
VR	Virtual reality
WHO	World Health Organization
WWWF	World Wide Web Foundation

Contents

List of figures

List of tables

List of boxes

Executive summary

This report examines cyber violence affecting girls and adolescents ([1]) in the European Union, analysing its prevalence, underlying drivers and consequences, and reviewing the effectiveness of existing policy and legal responses. It is based on a mixed-methods research design that combines legal and policy analysis, statistical evidence, and participatory insights from adolescents across ten EU Member States, providing a comprehensive understanding of both the structural and lived dimensions of cyber violence and supporting evidence-based policy action at EU and national levels.

The study was conceived as a bridge between research and policy, ensuring that empirical findings directly inform EU and national measures to prevent and respond to gender-based cyber violence.

The study explores how girls aged 13–18 define, experience and respond to cyber violence, both as victims and as bystanders, and considers the wider social and institutional contexts in which these experiences take place. The analysis of boys' (15-18) experiences focuses on social norms, masculinity, bystander behaviour, and empathy. Particular attention is given to the ways in which gender norms, social expectations and patterns of digital interaction shape young people's perceptions and behaviours online.

The research is framed within the Beijing Platform for Action, with a focus on Area D on violence against women and Area L on the girl child and supports EU efforts to prevent and address gender-based violence in all its forms.

Key Findings

Cyber violence against women and girls is increasingly recognised as an integral part of girls' everyday lives

- For many girls, cyber violence is not an occasional threat but a persistent feature of their daily lives, shaping how they communicate and engage online. Girls described constant exposure to harmful behaviours that make digital spaces feel unpredictable and unsafe.
- Cyber violence is part of everyday digital life, with harmful messages, insults, rumours and unwanted attention appearing daily or even hourly across platforms.

---

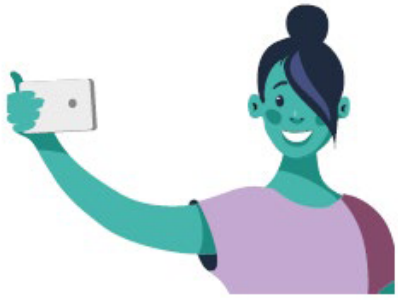
[1] Authors recognise that various terms are used to describe this phenomenon including technology-facilitated abuse, technology-facilitated gender-based violence, and technology-facilitated violence against women. For the purposes of this project, the term 'cyber violence' has been adopted, as it is the most commonly used within the European context and aligns with Directive (EU) 2024/1385 on combating violence against women and domestic violence.

Young people experience it as a continuum across online and offline settings, where harassment and exclusion often continue within schools or peer groups.

- Girls are targeted more frequently than boys, particularly through sexual harassment, image-based abuse and attacks on reputation. Repeated exposure to these behaviours contributes to a sense that cyber violence is unavoidable and difficult to escape, as girls come to see it as part of the online environment they must navigate.
- Discussions in focus group settings highlighted that boys often engage in cyber violence to gain social approval from peers. Boys highlighted how dominant norms of masculinity shape boys' online behaviour. Acts like non-consensual image sharing or group harassment are framed as performances to impress others or conform to peer expectations.

Girls are exposed to cyber violence from a young age

- Cyber violence begins when girls first start using digital technologies and social media, with many recalling early encounters with offensive or unwanted messages, sometimes before entering secondary school. Survey data confirm that unwanted messages and explicit content are among the most common forms of online abuse, with a significant share of girls reporting such experiences before the age of 15.



- Younger girls (13–15) report more relational and peer-based forms of aggression, including exclusion, gossip and body shaming, while older girls (16–18) more often face sexualised and coercive forms of abuse, such as online sexual coercion and extortion ([2]), deepfakes and non-consensual image sharing.
- Inappropriate or sexualised content appears even on platforms designed for children, showing that existing safeguards are insufficient. Girls called for earlier and age-appropriate prevention and digital literacy activities, noting that awareness sessions in schools often take place only after incidents have occurred.

([2]) Online sexual coercion and extortion of children is defined by Europol as a form of digital blackmail of children where sexual information or images are used to obtain sexual material, sexual favours or money from a victim (Europol, 2017). It is also a form of technology-facilitated gender-based violence often referred to colloquialy as 'sextortion' when affecting adult victims. It is important to note that this colloquial terms should not be used in cases affecting children.

Sexual and image-based abuse, including AI-generated deepfakes, is a growing and particularly harmful form of cyber violence

- Sexual and image-based abuse is one of the most visible and damaging forms of cyber violence, with participants describing these experiences as deeply distressing and harmful to their sense of safety, privacy and reputation. Non-consensual photos are often taken or shared within school or peer environments, spreading rapidly beyond girls' control.
- The creation and distribution of manipulated or AI-generated images ("deepfakes") is an alarming new form of abuse, used to humiliate or coerce girls and leaving them with little possibility of redress.
- The speed and reach of online sharing amplify the harm, as photos and videos can circulate widely in seconds. Even seemingly harmless images, shared voluntarily or with friends, can become a source of harassment or blackmail when used without consent or taken out of context.

Protections and institutional responses are not keeping pace with technological change

- Legal and policy analysis shows that protections against cyber violence remain fragmented and uneven across the EU. Directive (EU) 2024/1385 on Violence against women and domestic violence is a major step forward and prioritising its full transposition into national law and implementation is key to bring out significant positive results to women and girls' lives.
- Girls often perceive schools, police and other authorities as ill-prepared or unresponsive, reporting that their complaints are sometimes dismissed or ignored. Fear of blame, shame and lack of confidence in adults' ability to act effectively discourage many from reporting, leaving victims to handle harm on their own.
- Weak and inconsistent moderation practices allow harmful content to circulate widely, while online anonymity enables perpetrators to act with impunity. In line with the Digital Services Act (DSA) provisions, stronger coordination between EU and national authorities, alongside binding accountability for digital platforms, is needed to ensure that technological progress is matched by adequate legal and institutional protection.

Peer culture and gender norms strongly influence the occurrence of cyber violence and the ways it is addressed

- Peer culture plays a crucial role in shaping how online violence unfolds and how young people respond to it. Harmful behaviours are often reinforced by social pressure to conform or maintain status, particularly among boys, and by gender norms that encourage victim-blaming and double standards.

- Cyber violence reflects broader gender inequalities, with humiliation and control used to police girls' appearance, behaviour and online self-expression. Bystander inaction also sustains abuse: most adolescents have witnessed online violence without intervening, often out of fear or uncertainty.
- Intersectional factors such as age, race, disability, belonging to a religious minority but also sexual orientation and gender identity or body size increase vulnerability, compounding the risks for some groups of girls. Participants called for inclusive and participatory prevention efforts, involving boys and promoting empathy, respect and accountability.
- Good practices identified through national and EU-level mapping show that gender-transformative education and dialogue-based approaches can challenge harmful norms, empower bystanders and reduce tolerance for online abuse.

Introduction

Across the European Union, cyber violence has emerged as a rapidly expanding form of gender-based violence that affects adolescents with particular intensity. As digital communication becomes deeply embedded in young people's social lives, online spaces increasingly shape how relationships are formed, negotiated, and sometimes exploited. Recent EU-level analyses show that women and girls are disproportionately exposed to intrusive, sexualised, or hostile behaviours online (*EIGE 2022b*), reflecting enduring gender norms and the shifting dynamics of peer interactions in digital environments.

With the rise of digital connectivity and the increased centrality of social media in adolescents' lives, the risk of technology-enabled harassment, non-consensual image sharing, cyberstalking and hostile online behaviours has intensified (*Council of Europe 2018*). At the same time, European and international institutions have progressively recognised online gender-based violence as a pressing policy challenge (*UN Special Rapporteur on VAWG 2018; European Parliament 2021a*), highlighting its social and political relevance and its implications for children's rights, mental health, and gender equality.

The existing datasets and institutional reports highlight the scale and diversity of online abuse. Yet, far less is known about how adolescent girls understand and interpret these behaviours in their everyday lives, how they respond when harm occurs, and what support mechanisms they find meaningful, trustworthy, or insufficient. By adopting a qualitative, participatory approach, this study explicitly positions adolescents as knowledge-holders rather than passive respondents—a methodological choice that enables their voices, perceptions, and lived experiences to be meaningfully captured and foregrounded. They provided most valuable evidence for the EU and national level policy action.

The main objective of the study is to advance knowledge on how adolescent girls aged 13-18 experience cyber violence in the EU. This involves examining the ways in which they define and recognise cyber violence - both as victims and bystanders - while also analysing their perceptions of institutional and adult-led prevention efforts, and their experiences of reporting incidents to parents, teachers, or online platforms. In doing so, the research not only sheds light on girls' direct encounters with cyber violence, but also on their evaluations of available support mechanisms and their reflections on their own behaviour online. Discussions with adolescent boys reflects their awareness of how cyber violence affects girls and touched upon how they can behave when witnessing it.

The study adopted a multi-layered methodological approach combining desk research and fieldwork in order to capture both the structural dimensions of the phenomenon under investigation and the lived experiences of those directly concerned. Triangulation across data

types - quantitative evidence, policy and legal frameworks, and participatory insights - ensured both breadth and depth ([3]).

Desk research and literature review provided the conceptual and empirical foundation for the qualitative research. Policy and legal mapping of international, EU, and national frameworks helped to identify how cyber violence is regulated. Official sources were complemented by snowball techniques to capture emerging national measures, providing a comparative overview of legal and policy responses across Member States (MS). Statistical data analysis contextualised the phenomenon using EU-level and national surveys, comparative studies, and EU-funded projects such as EU Kids Online. They helped quantify trends and connect structural data with qualitative findings.

The second pillar of the methodology was qualitative fieldwork through focus groups, capturing adolescents' lived experiences. Across 10 EU MS (Belgium, Cyprus, Estonia, Germany, Ireland, Italy, Poland, Romania, Spain, and Sweden), 37 focus groups involved 133 girls (13–18). Focus group discussions with 38 boys aged 15 to 18 also took place in three EU MS (Cyprus, Ireland and Romania). Age-appropriate guides included interactive tools for younger groups and scenario-based discussions for older participants; boys' groups focused on social norms, masculinity, bystander behaviour, and empathy.

Chapter 1 presents the conceptual and contextual foundations of cyber violence, including definitions, main forms, and prevalence data at international, EU and national level. Perceived causes and contributing factors are also analysed. Chapter 2 presents the findings from the qualitative fieldwork, highlighting the awareness and understanding of cyber violence of girls and boys who took part in the focus groups across ten MS. Chapter 3 explores in more detail girls' experiences of cyber violence, including the contexts, roles, and dynamics involved. Chapter 4 examines the impacts of cyber violence on young people, highlighting their own perspectives on its social and psychological consequences. Chapter 5 addresses prevention and responses, reviewing some examples of international, EU, and national frameworks and policy measures, and young people's views on their effectiveness. Finally, the report concludes with key insights and policy implications, outlining recommendations for future EU and national action.

[3] For a more detailed description of the methodology, see Box 7 in the Annex.

1. The phenomenon of cyber violence against girls and young women

1.1. Concepts and definitions of cyber violence

Cyber violence against women and girls (CVAWG) constitutes a multifaceted and intersectional form of gender-based violence (GBV), encompassing behaviours such as cyberstalking, online sexual harassment, non-consensual image sharing, and gendered hate speech. These harms are shaped by societal norms that reinforce male dominance, relational dynamics like coercion and peer validation, and developmental factors that make adolescents especially vulnerable to online abuse (Cybersafe Project, 2020). Although academic discourse on cyber violence dates back to the mid-1990s [4] - coinciding with the rise of internet usage and online platforms - wider recognition of CVAWG has only received sustained attention in recent years. Earlier studies explored how technology reshaped dominant paradigms around gender, identity, and sexuality (Gurumurthy, 2009), raising concerns about its role in enabling new forms of violence, particularly against women. As Judy Wajcman (2004, 2010, 2015) has argued, technology is deeply embedded in social power relations, and far from neutral—it reproduces and reconfigures gendered hierarchies that can sustain symbolic and structural forms of violence.

Given its rapidly evolving nature, cyber violence is classified in various ways, taking into account the type of the behaviour, the characteristics of victims and perpetrators, the technological tools used, and the resulting impacts (Mukred et al., 2024). Other key elements in conceptualising it include the victim-survivor's perception of harm and the lack of consent (Koukopoulos et al., 2025).

CVAWG covers a wide spectrum of online harms, including stalking, bullying, doxing, trolling, sexual harassment ([5]), defamation, hate speech, and exploitation ([6]). Victims are often children, adolescents, and women, with certain groups disproportionately affected and targeted. Perpetrators may act individually, collectively or through organisations, making use of platforms such as social media, messaging apps, email, phone communications, and other digital channels.

The continuously evolving nature of cyber violence poses significant challenges for the development of conceptual and legal definitions. Its scale and speed make it one of the most pervasive and severe forms of violence in contemporary society (USAID, 2023). To enhance understanding and better reflect its complexity, the Council of Europe (CoE) proposed a

---

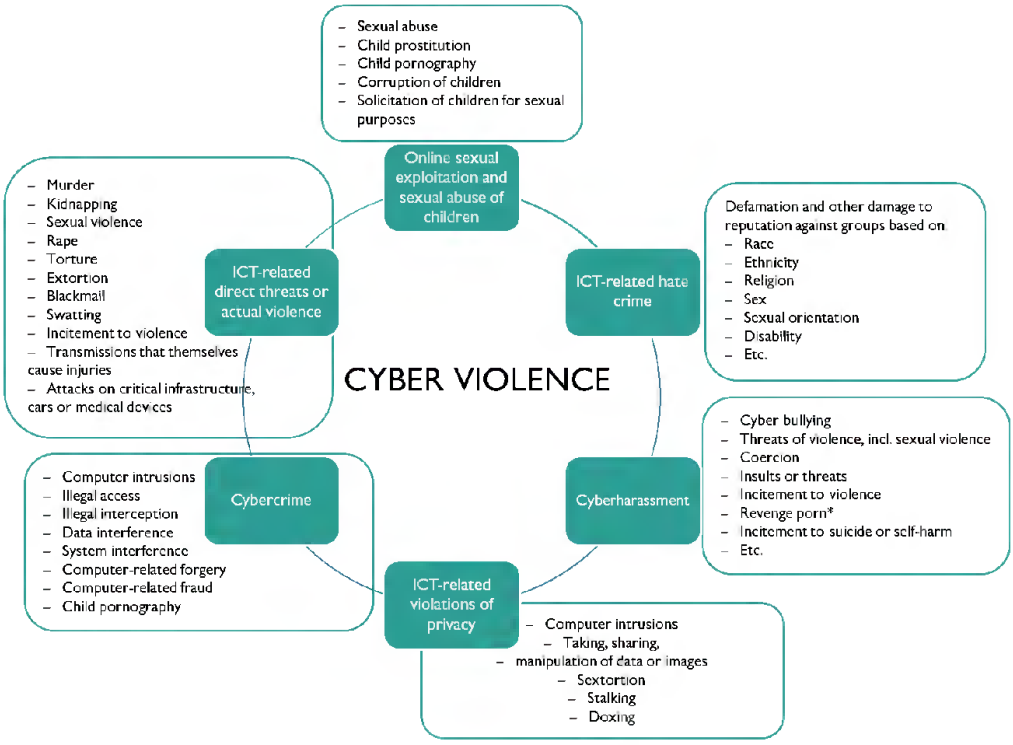
[4] For example, early studies on cyber violence - such as McGraw's *Sexual Harassment in Cyberspace: The Problem of Unwelcome E-mail* (1995) and Adam's *Cyberstalking and Internet Pornography: Gender and the Gaze* (2002) - offer insights into the phenomenon and its consequences.

[5] This term covers a wide range of situations such as image-based sexual harassment including creepshots, upskirting, non consensual image or video sharing, cyberflashing, deepfakes, recorded sexual assault and rape.

[6] This term covers a wide range of situations such as scamming for financial gain/extortion, grooming children or young people towards sexual activity, or criminal activity.

multi-dimensional framework for cyber violence (Council of Europe, 2018) which categorises various forms of online harm, such as information and communication technologies (ICT)-related privacy violations, cyber harassment, hate crimes, and online child exploitation (Figure 1).

Figure 1: CoE's conceptual framework of cyber violence



* The term 'revenge porn' is commonly used in the legal and policy frameworks of Member States, whereas academic literature generally refers to 'non-consensual sharing of intimate images'. 'Revenge porn' can be misleading, as it downplays the severity of the crime, the different range of gender sexualised forms of abuse, and its profound impact on victims.
Source: Council of Europe, 2018, p. 6.

At the policy level, EU policy documents began referring to the United Nations' (UN) definition of cyber violence, as outlined in the 2018 report by the UN Special Rapporteur on Violence against Women and Girls (United Nations, 2018). The report defines cyber violence as *gender-based violence against women that is committed, assisted or aggravated in part or fully by the use of ICT, such as mobile phones and smartphones, the Internet, social media platforms or email, against a woman because she is a woman, or affects women disproportionately.*

This definition was reaffirmed in the 2021 European Parliament Resolution on cyber violence (European Parliament, 2021a). A major legislative step followed with the adoption

of the 2024 EU Directive on Combating Violence Against Women and Domestic Violence. As the first comprehensive EU law addressing violence against women, the Directive criminalises a wide range of cyber offences, including the non-consensual sharing of intimate or manipulated material, cyberstalking, cyber harassment, cyber flashing, cyber incitement to violence or hatred and online sexual harassment. It thus serves as a key legal foundation for defining and tackling cyber violence across the EU, recognising its complexity and evolving nature. Beyond providing a much-needed definition, the Directive also includes several instrumental provisions on cyberviolence, such as the obligation to take down content, the definition of appropriate reporting channels and the need for Member States to provide specialist support services for victims of cyberviolence. Considering the above, Box 1 below outlines the most frequent forms of cyber violence.

Box 1: Most frequent forms of cyber violence

- **Cyber harassment:** including cyberbullying, online sexual harassment, the unsolicited receipt of sexually explicit material, mobbing and dead naming. According to the 2024 EU Directive, cyber harassment includes (i) repeatedly or continuously engaging in threatening conduct directed at a person, at least where such conduct involves threats to commit criminal offences, by means of ICT; (ii) engaging, together with other persons, by means of ICT, in publicly accessible threatening or insulting conduct directed at a person; (iii) the unsolicited sending, by means of ICT, of an image, video or other similar material depicting genitals to a person, (iv) making accessible to the public, by means of ICT, material containing the personal data of a person, without that person's consent.
- **Cyberstalking**: intentional conduct of repeatedly or continuously placing a person under surveillance, without that person's consent or a legal authorisation to do so, by means of ICT, to track or monitor that person's movements and activities.
- **ICT-related violations of privacy**: including the accessing, recording, sharing, creation and manipulation of private data or images, specifically, including image-based sexual abuse non-consensual creation or distribution of private sexual images, doxxing and identity theft;
- **Recording and sharing images of rapes or other forms of sexual assault;**
- **Remote control or surveillance:** including by means of spy applications on mobile devices;
- **Threats:** including direct threats and threats of and calls to violence, such as rape threats, extortion, online sexual coercion and extortion (sextortion), blackmail directed at the victim, their children or at relatives or other persons who support the victim and who are indirectly affected;
- **Sexist hate speech:** including posting and sharing content, inciting to violence or hatred against women or LGBTQ+ people on the grounds of their gender identity, gender expression or sex characteristics;
- **Inducements to inflict violence on oneself:** such as suicide or anorexia and psychic injury;
- **Computer damage:** to files, programmes, devices, attacks on websites and other digital communication channels;
- **Unlawful access:** to mobile phones, email, instant messaging messages or social media accounts;
- **Breach of the restrictions on communication**: imposed by means of judicial orders;
- **The use of technological means for trafficking in human beings:** including for sexually exploiting women and girls.

Source: European Parliament Resolution, 2021

In light of these definitions, inconsistencies in terminology across legal and academic contexts highlight the need for broad interpretations that can capture the diverse forms and expressions of violence (EIGE, 2022b).

While cyber violence can target any individual or group and encompass a variety of actions and behaviour, it disproportionately affects women and children (Council of Europe, 2018). Moreover, while men can also experience cyber violence, research (e.g., Backe et al., 2018; Hicks, 2021) shows that women and girls face greater risks due to entrenched gender norms and inequalities, often experiencing more severe and lasting consequences (EIGE, 2022b). Given that younger individuals are the most active users of social media and ICT, international research ([7]) has highlighted that girls and young women face heightened vulnerability to specific forms of cyber violence, including but not limited to cyberbullying and the non-consensual sharing of intimate images. This underscores the need for a child-centred approach ([8]), that considers how psychological, developmental, and societal factors influence young people's digital interactions (Cybersafe Project, 2020).

Building on this understanding, the present study adopts a comprehensive view of CVAWG to reflect its multifaceted nature. Box 2 presents the forms of CVAWG which were considered in the analysis.

Box 2: Forms of CVAWG considered for this research study

- ✓ **Cyber harassment (including cyberbullying)**
- ✓ **Cyberstalking**
- ✓ **Non-consensual sharing of intimate or manipulated material**
- ✓ **Cyber incitement to violence or hatred directed at women and girls**

These forms of cyber violence are outlined in the 2024 EU Directive on Combating Violence Against Women and Domestic Violence and are recognised as the most widespread forms of cyber violence (EIGE (2022b).

1.2. Prevalence and contexts of cyber violence

CVAWG is increasingly recognised as part of a broader continuum of violence that includes both online and offline behaviours (Dunn, 2020; Lu et al., 2021; Machado et al., 2022). It is grounded in structural power imbalances and perpetuated by societal gender stereotypes (EIGE, 2024). Many forms of cyber violence, such as harassment, bullying, and stalking, often originate in offline interactions, with the digital environment amplifying their scope and impact.

In a world where digital technologies are embedded in everyday life the internet and related tools have become extensions of the environments in which women and girls experience violence. This digital dimension also has direct consequences for their safety, dignity, and overall well-being (OAS, 2021). For instance, street harassment, bullying at school, and

---

[7] See, for instance: PLAN International, 2020; Vogels, 2022; Sciacca et al., 2023.

[8] See Council of Europe, 2020. Additional literature on this topic is available in the Council of Europe's library, which features research on cyber violence categorised by target group, including studies focused specifically on children. See, for instance: WeProtect Global Alliance, 2020; WeProtect Global Alliance, 2021. For more information, please visit: CoE Library on Cyberviolence

intimate partner abuse may extend into digital spaces through cyber harassment, cyber bullying, and non-consensual image distribution and online stalking. Conversely, online interactions with strangers on social media can be exploited by perpetrators and escalate into real-world threats, including sexual violence. These patterns of abuse underscore the link between digital and physical violence against women and girls (OAS, 2021).

Studies reveal this significant overlap between cyber violence and offline abuse; for example, 70% of victims of cyber harassment and stalking in the EU have also endured intimate partner violence, as shown by the EU Agency for Fundamental Rights (FRA) (European Union Agency for Fundamental Rights, 2015). This overlap underscores the pervasive nature of CVAWG and how it is embedded within broader patterns of systemic violence.

Moreover, ICTs have played a significant role in enabling new strategies of abuse and control, particularly within intimate partner violence. Among young couples, such behaviours have become normalised within online-offline interactions and are often misinterpreted as signs of love (Lu et al., 2021). Such online abuse includes demanding access to a partner's passwords, monitoring their online activities, and restricting their interactions on social platforms.

Research consistently shows that, among women, sexual harassment and stalking are the most commonly reported forms of cyber violence (UN Women and World Health Organization, 2023). A particularly alarming aspect of online harassment is its potential for widespread distribution beyond the control of either the sender or recipient. In extreme cases, the creation and sharing of sexual images involving minors constitute child sexual abuse material (Smahel et al., 2020).

The EU-GBV survey data (Wave 2021) ([9]) further indicate that receiving unwanted messages or emails is the most widespread form of (cyber) violence by the same perpetrator repeatedly (9%), surpassing public offensive comments (4%) or image-based abuse (1%) (Figure A.7 in Annex). Notably, some victims reported such experiences before the age of 15, further highlighting that exposure to violence begins in childhood (Figure A.8 in Annex).

Testimonies from young participants in this study's focus groups further confirm that even seemingly harmless images – such as a swimsuit photo – can trigger harassment, blackmail, or long-term reputational harm, reflecting research that highlights how content can quickly escape control once shared.

---

[9] The EU-GBV survey (wave 2021) includes results covering the 27 EU Member States. In total, the estimated EU-27 average results are based on data collected from 114 023 women (18–74 years of age) across the EU. The data collection took place between September 2020 and March 2024. Eurostat coordinated the data collection in 18 Member States, and the national statistical authorities of these countries carried out the survey. Italy agreed to share the data from its national survey to provide comparable data for the main indicators. For the remaining eight Member States, FRA and EIGE took responsibility for the data collection following the Eurostat methodological manual. More details on the survey methodology, available at https://ec.europa.eu/eurostat/cache/metadata/en/gbv_sims.htm.

Research also indicates that age, alongside gender, plays a crucial role in the occurrence of cyber violence (FEMM Committee, 2018; Pichel et al., 2021; López-Castro et al., 2023; Schittenhelm et al., 2024). Social media use is most prevalent among girls and young women, and less common among older women. For younger women and girls these platforms serve multiple purposes, including maintaining friendships, communicating with family, exploring job opportunities, and engaging with wider social networks. Yet, women do not need to be active internet users to experience cyber violence or abuse. They may still be targeted, for example through the online distribution of sexual content or sexual exploitation on trafficking websites (FEMM Committee, 2018).

A 2020 global survey by the World Wide Web Foundation (WWWF) and Girl Guides [10] found that 52% of young women and girls reported experiencing some form of online abuse. Notably, respondents aged 15 to 19 expressed particular concern over the unauthorised sharing of private images and videos. Similarly, Plan International (PLAN International, 2020) has estimated that 58% of young women and girls worldwide have experienced online harassment on social media platforms, noting that most girls report their first experience of social media harassment between 14 and 16 years of age.

Male teenagers and young men are found to be specifically targeted for online sexual coercion and extortion, often referred to as 'sextortion' (Thorn, 2024, WeProtect, 2024). In such cases, victims face blackmail or threats of intimate images being shared. Such pictures or videos can have been shared by the victims or AI-produced. Predators then demand sexual favours or sexual content and most often money from the victim in exchange for not disseminating the images. Evidence from various countries points to perpetrators operating in organised criminal networks often based in developing countries with financial gain being the main motivator (Europol, 2017). With free generative AI tools becoming widely available, predators easily use some of the victims' photos or videos posted on social media and turn them into deepfake images and videos (WeProtect, 2024). Evidence from the UK, the USA and Australia show increases over the past few years in the number of cases of teenage boys facing such violence (Governement of Australia, 2022,

Evidence at the EU level supports these findings, showing how risks of cyber violence vary by both age and gender. According to data by the World Health Organization (WHO), cyberbullying is most prevalent among both boys and girls at age 13 across most EU countries and regions. As seen in figure A.1 and figure A.2 in Annex, WHO's 'Health Behaviour in School-aged Children' (HBSC) study (Cosma et al., 2024) indicates that, in 2022, a higher percentage of 13-year-old girls experienced cyberbullying than boys in nearly all EU MS (22 countries) as well as in both the French and Flemish regions of Belgium. This

[10] A global survey was conducted in 2020 by WWWF and World Association of Girl Guides and Girls Scouts using UNICEF's Report platform concerning young people's experience of online abuse and harassment. There were 8 109 respondents of which 51% female and 49% male. Survey data is available at https://ureport.in/opinion/3983/

gender gap is also observed among 15-year-olds, with girls reporting higher rates of cyberbullying in 15 EU MS and in both Belgian regions.

Among 13-year-old girls, the prevalence of cyberbullying ranges from 10% in Portugal and the Netherlands to 29% in Latvia. For boys of the same age, rates range from 7% in the French region of Belgium to 32% in Lithuania. Among 15-year-olds, the variation is similar: for girls, reported rates range from 7% in Portugal to 24% in Spain, while for boys, they range from 3% in Spain to 31% in Lithuania.

While earlier research suggested that incidents of cyber harassment were more prevalent in countries with higher internet access rates (European Union Agency for Fundamental Rights, 2015), this link has become less relevant over time. Since 2015, disparities in internet access across EU countries have significantly diminished ([11]), indicating that cyber violence is now a widespread issue regardless of connectivity levels.

Additionally, although social media enhances communication and fosters social connections, its excessive or compulsive use may negatively impact the well-being of children and adolescents in particular. Social media use among adolescents reflects gendered patterns, with more girls than boys actively engaging with these platforms between the ages of 11 and 19 (Leonhardt and Overå, 2021). In addition, evidence indicates that girls experience stronger negative psychological effects linked to social media engagement.

For example, girls aged 11–13 are more likely than boys to report poorer sleep, body image concerns, and depressive symptoms (National Academies of Sciences, Engineering, and Medicine, 2024).

Excessive social media use among girls has been associated with vulnerability to depression and anxiety, largely due to societal pressures related to self-evaluation, body image, and conforming to beauty standards. These pressures can contribute to dissatisfaction, emotional distress, and low-esteem (Sala et al., 2024). Research further shows that susceptibility to these negative effects varies by age and gender: girls aged 11–13 and boys aged 14–15 show greater risk of decreasing life satisfaction as social media engagement increases (National Academies of Sciences, Engineering, and Medicine, 2024).

Findings from the HBSC study provide additional evidence of this association, highlighting concerns related to 'problematic social media use' - defined as exhibiting addictive-like symptoms [12]. As seen in figure A.3 and A.4 in Annex, in nearly all EU MS in 2022, girls were more prone than boys to report such problematic use at both ages 13 and 15, with the exception of Finland ([13]). Among 15-year-olds, the lowest percentage of girls exhibiting

---

[11] Please see Eurostat data on level of internet access, available at: https://ec.europa.eu/eurostat/databrowser/view/tin00134/default/table?lang=en

[12] Please find the HBSC database on social media use at: https://data-browser.hbsc.org/measure/problematic-social-media-use/

[13] In Finland, boys aged 15 were more likely than girls to indicate problematic social media use (12% compared to 8%).

symptoms of problematic social media use was observed in the Netherlands and Denmark (7% in both), while Romania had the highest rate at 28%. For boys, the lowest rates of reported 'problematic social media use' were also found in the Netherlands, Hungary, and Latvia (3%), with Romania again showing the highest rate at 18%.

As seen in Box 2, at national level, several MS have conducted specific surveys on cyber violence to better understand its prevalence, groups affected, and consequences.

Box 3: Examples of surveys on cyber violence carried out in EU MS

- **France:** A 2022 survey by Feminists Against Cyber Harassment ([14]) found that the majority of respondents victims of cyber violence were women (84%) and individuals who experienced online discrimination based on gender identity and sexual orientation (43%). People with disabilities and religious minorities also faced disproportionate risks and greater barriers to reporting.
- **Slovenia:** The ClickOFF! project (2024) (Šulc, A. et al., 2024) found that over 50% of girls aged 13+ had experienced cyber violence ([15]). Older students reported higher rates of both victimisation and perpetration. Among primary school students, 15–16-year-olds reported the highest rates of victimisation (57%), while 15-year-olds were most likely to perpetrate (10%).
- **Netherlands:** Dutch Central Bureau of Statistics (CBS) data (2022/2024) ([16]) shows that 1 in 5 young people (15–24) experienced online threats, bullying, stalking or the non-consensual distribution of images. In 2024, 22% of girls aged 16–18 reported online sexual harassment, compared to 7–8% of boys ([17]). Regarding offline sexual harassment, the data further revealed that young women are disproportionally affected ([18]).
- **Portugal:** The Portuguese Association for Victim Support (APAV) ([19]) reported data from the Safe Internet Line, which has been operated by APAV since 2019. In 2019, the helpline recorded 827 cases related to online sexual violence, of which 676 involved child pornography. Moreover, most of the cases reported to the APAV hotline for support against cybercrime involved young people aged 11 to 17.
- **Belgium:** The 2022 #YouToo? survey ([20]) found 1 in 5 young people had experienced cyberbullying, often starting at an early age, indicating a need for early digital literacy and prevention. In 2026, a study on cyber violence in the context of dating found that 66% of respondents reported being pressured to send nude photos on dating apps and that 60% of respondents who did sent a nude photo via an online dating site when then threatened with its distribution ([21]).
- **Italy:** A 2023 'Osservatorio Indifesa' survey ([22]) showed that nearly 80% of adolescents viewed the internet as unsafe. Top concerns included cyberbullying (23%), identity theft, and social isolation (18% both), and other issues such as non-consensual intimate image abuse (14%), harassment (10%), and stalking (7%).
- **Germany:** The 2024 Cyberlife study by *Bündnis gegen Cybermobbing* (Alliance Against Cyberbullying) ([23]) found that 2 million students had experienced cyberbullying. Key issues included low awareness among

---

([14]) Cyberviolence et cyberharcèlement: le vécu des victimes
([15]) ClickOFF! project
([16]) 2.2 million cybercrime victims in 2022 - Statistics Netherlands
([17]) Prevalence Monitor on Domestic Violence and Sexually Transgressive Behaviour 2024 - Statistics Netherlands
([18]) *Ibid.*
([19]) Violência Sexual Online
([20]) Cyberbullying: One in five young people in Belgium have been victims - The Brussels Times
([21]) Les violences numériques dans le contexte du dating et des relations entre (ex-)partenaires en Belgique | Institut pour l'égalité des femmes et des hommes
([22]) Online Violence: Protection and Prevention of Minor Victims - Terre des hommes
([23]) Tension Between Fascination and Danger: Cyberbullying Among School Students - Cyberlife

parents and schools, and heightened vulnerability among socially isolated youth. Alarmingly, one in four affected students had suicidal thoughts, with suicide a leading cause of death among 15–25-year-olds.

1.3. Perceived causes and contributing factors

Cyber violence is deeply rooted in broader social structures, gender norms, peer dynamics, and the rapidly evolving digital landscape. It is not only shaped by the behaviour of individuals but also by structural inequalities that make certain groups more vulnerable. **Key underlying causes include unequal power relations between women and men, gender stereotypes, and the lack of effective safeguards in online platforms.** Age and other intersecting factors such as socio-economic status, minority identity, or disability can also significantly influence both exposure to and the impact of cyber violence. Adolescents, for example, are at greater risk as they navigate social development, increased online engagement, and peer pressures, while girls and young women disproportionately face sexualised forms of online abuse. Persistent gender stereotypes and norms, including societal expectations about how women and men should look, behave, or express their sexuality, normalise certain forms of online harassment and are often used to justify and downplay abuse.

Early instances of cyberbullying are frequently dismissed by children themselves as jokes or harmless fun. Younger children, in particular, may not recognise these behaviours as cyberbullying, perceiving them instead as tolerable - especially when the actions lack perceived malicious intent (Baas et al., 2013). **This minimisation normalises harmful behaviours and delays recognition of abuse as a serious issue.** However, three key characteristics differentiate cyberbullying from innocent pranks or playful interactions: intention, repetition, and power imbalance (Baas et al., 2013).

Adolescents aged 15 to 16 report higher exposure to and receipt of online sexual content than their younger peers aged 12 to 14, with girls experiencing this more frequently than boys. As seen in figure A.9 in Annex, at EU level there is a significant correlation between age and the receipt of sexual messages. In every EU country represented, a higher percentage of youth in the oldest age group (15-16 years old) compared to the other age group (12-14) reported receiving this type of messages. This highlights how greater online activity, coupled with gendered expectations about female sexuality, increases risks and exposure for older adolescent girls in particular. As illustrated in figure A.10 in Annex, in most EU countries represented except for Croatia and Malta, girls are more affected by unwanted sexual requests than boys.

Age is therefore a significant contributing factor, as developmental transitions during adolescence heighten both digital engagement and vulnerability to cyber violence. Older adolescents, who are more active online and are more likely to engage in risk-taking behaviours, face greater exposure to sexualised interactions. This increased risk is compounded by social expectations around sexuality, gendered double standards, and peer

validation practices. Indeed, while exposure to sexual content is increasingly seen as a normal part of adolescent sexual development, it also heightens the risk of cyber violence (European Parliament, 2024b).

Findings from the EU-GBV survey confirm these age-related differences in exposure to cyber violence. Younger women report a higher prevalence of image-based abuse, such as the non-consensual publication of photos, videos, or personal details. For instance, 37% of women aged 25–34 and 23% of those aged 18–24 reported such experiences, compared to just 3% among women aged 55–74. On the other hand, among the types of (cyber) violence experienced by older women (from 55 years old and above), the most common was the offensive or embarrassing public comments (Figure A.6 in Annex). **These patterns indicate that age, life stage, and type of digital engagement are important drivers shaping different risks across groups.**

As with all forms of GBV, CVAWG is also shaped by a variety of other intersecting factors that exacerbate vulnerability and marginalisation in digital spaces. These include disability, sexual orientation, political beliefs, religion, social background, migration status, and even celebrity status (GREVIO, 2021). **Such intersecting identities can compound discrimination, making cyber violence both more frequent and more harmful.**

Numerous studies emphasise the intersectional nature of CVAWG, revealing that women and girls with diverse identities and backgrounds often face heightened risks of online abuse. For instance, FRA (European Union Agency for Fundamental Rights, 2015) found that 34% of women with disabilities reported experiencing physical, sexual, or psychological violence, including online threats, compared to 19% of women without disabilities. Disability-related stigma, barriers to reporting, and isolation further intensify the harm.

Ethnicity and minority status also significantly influence risk of online abuse. A 2017 FRA study (European Union Agency for Fundamental Rights, 2017) focusing on minorities indicated that younger migrants experience more in-person and online harassment than older migrants. Among migrants and minorities, these forms of harassment erode trust in institutions and hinder social integration (European Union Agency for Fundamental Rights, 2015). Young people's perspectives during focus groups add a lived dimension to these findings, as several described how racism and visible expressions of faith make them targets online. Thus, prejudice and systemic racism are powerful contributing factors.

From the perspective of children and young people, factors such as race, religion, ethnicity (Ratajczak and Galzignato, 2019), social class, disability, sexual orientation, and gender identity increase risk to online harm (Project deSHAME, 2017). Studies confirm that adolescent girls from disadvantaged socioeconomic backgrounds, minority groups, or with disabilities are disproportionately affected. For example, Wallace et al. (2023) found that about 40% of the variance in cyber violence victimisation among girls aged 14-18 is attributable to intersectional factors. Similarly, Pew Research Center data (Vogels, 2022) show that experiences of cyberbullying among U.S. youth vary not only by age but also by

physical appearance, ethnicity, sexual orientation, and political beliefs. These findings highlight how personal identity markers interact with societal power dynamics to shape patterns of risk. Recent findings from Belgium found that young adults and LGBTQIA+ people are particularly vulnerable to online violence on dating apps due to their greater use of digital tools in relationships and dating, which fosters certain forms of online violence. For LGBTQIA+ people, this violence can also be compounded by specific risks, such as outing or the exploitation of sensitive personal data, further increasing their vulnerability (Institut for l'égalité des Femmes et des Hommes, 2026).

Vulnerabilities can also arise from personal circumstances, such as family challenges, previous abuse, or gang involvement (Project deSHAME, 2017). The HBSC study (Cosma et al., 2024) indicates that peer cyber violence often reflects socioeconomic circumstances, with children from families of low affluence being more likely to be affected by cyber violence. However, this pattern is not observed in all countries in the EU. In several countries and regions, the prevalence of cyber violence is higher among children of families with high affluence [24]. Moreover, problematic social media use and cyberbullying do not show significant variation across family affluence groups (Table A.7 in Annex).

Chapter 1 mapped the conceptual landscape of cyber violence against girls and young women, highlighting its forms and prevalence. Yet, these dimensions only partially capture how such violence is experienced in daily life. To complement this body of evidence with lived realities, the study engaged directly with adolescents. As part of this research, focus groups were conducted with girls and boys in Belgium, Cyprus, Germany, Estonia, Spain, Ireland, Italy, Poland, Romania, and Sweden to explore how young people - particularly girls - perceive, define, and experience cyber violence. These discussions provided crucial first-hand insights, encompassing both personal experiences and observations of peers. Focus group findings are integrated throughout the following sections, where young people's voices are used to illustrate and expand on existing evidence. In doing so, the following chapters shift the lens from theoretical frameworks to lived realities, amplifying the perspectives of girls and boys and linking their experiences to the broader body of research.

[24] As shown in Table A.6 in Annex: For boys, this is the case of Poland, Estonia, Slovenia, Czechia, France. For girls: Estonia, Sweden, Czechia, Slovakia, Flemish Belgium. In these countries there is a significant difference in the prevalence by group of family affluence (at $P < 0.05$), for girls and/or for boys.

2. Perceptions of cyber violence among girls and boys

2.1. Experience and understanding of cyber violence

As anticipated before, cyber violence is a pervasive and rapidly evolving threat that disproportionately affects children, teenagers, and young adults - particularly girls - whose developmental stage and gaps in legal protection can heighten the harm they experience. (EIGE, 2022b). Cyber violence manifests in various forms, including verbal harassment, psychological manipulation, reputational attacks, and technology-enabled sexual abuse. Understanding these diverse forms is essential for young people to recognise abusive behaviours and respond effectively.

Young people's experiences and understandings of cyber violence differ significantly by age and gender (Pew Research Center, 2022). This variation is further explored through girls' own accounts in focus group discussions, as detailed in the sections below. Older girls, for instance, are more likely to encounter invasive and sexually explicit forms of abuse, such as receiving unsolicited explicit images, the non-consensual sharing of explicit images, and persistent inquiries about their whereabouts and activities from individuals other than their parents. In contrast, younger girls tend to face offensive name-calling and the spreading of false rumours about them (Table A.4 in Annex). This progression suggests that, as girls grow older, the cyber violence they experience becomes increasingly sexualised, and controlling. Moreover, these patterns align with girls' own descriptions of public humiliation, social exclusion, and appearance-based judgment, showing that cyber violence evolves in complexity as girls mature.

Technology-facilitated intimate partner violence as a growing concern

An emerging focus of research on cyber violence targeting girls and young women is technology-facilitated intimate partner violence. This form of abuse is characterised by actions such as control, harassment, stalking, and mistreatment of a partner through technology and social media (Zweig et al., 2014). Such form of intimate partner violence may occur within both current and former relationships, and it can manifest in emotional, physical, or sexual forms. Perpetrators use a wide range of digital methods: unauthorised access to email or social media accounts, GPS tracking and use of stalkerware, emotional manipulation, and online threats are all common. The use of 'smart' home devices for surveillance and stalking as well as AI tool is also common. Notably, these behaviours often continue even after the relationship has ended.

Technology-facilitated intimate partner violence is often intertwined with offline forms of dating violence, with both forms often occurring simultaneously (Van Ouytsel et al., 2020). Young people - particularly young women - may struggle to recognise these behaviours as abusive, complicating efforts to identify and address them.

Findings from the EU-GBV survey confirm these patterns: about one in nine women reported being pressured by a partner to disclose their whereabouts or being digitally tracked (via GPS, phone, or social networks). When distributing by age, the occurrence is particularly high among women aged 35-44, where nearly one in four (23%) reported such experiences (Figure A.5 in Annex).

Coercion to share sexual images is widespread

European data from the DeSHAME project (Project deSHAME, 2017) in Denmark, Hungary, and the United Kingdom, shows that one in ten respondents aged 13 to 17 (9% in DK, 7% in HU, and 12% in the UK) reported being pressured by a boyfriend or girlfriend to share nude images, with girls disproportionately affected. Additionally, 1 in 6 respondents (16%) reported having kept a screenshot of a nude or sexually explicit image or conversation for future use (13% in DK, 19% in HU, and 16% in the UK). Furthermore, 44% of respondents acknowledged that young people may engage in online sexual harassment as a form of revenge against an ex-partner (51% in DK, 33% in HU, and 47% in the UK). Similar findings are illustrated by the CYBERSAFE project which, through focus groups with young people aged 13-17 in Italy, Greece, Northern Ireland, and Estonia, found that online partner violence - especially male-controlled abuse against females - is frequently discussed among teenagers (Cybersafe project, 2020).

Anonymity online increases risks for vulnerable groups

The anonymity provided by digital platforms allows individuals to easily conceal their identity, putting young women, girls, and sexual, gender, and ethnic minorities at greater risk (Smith, 2023). Focus group participants echoed these concerns, reporting stalking, fake profiles, and the persistent monitoring of personal digital spaces as everyday threats. The ease with which people can create fake profiles or impersonate others in online spaces heightens the risks for those seeking connections, making these environments inherently unsafe and potentially violent with emotional consequences (Smith, 2023). Moreover, the digital nature of online abuse can lead young people to underestimate its impact, believing that simply logging off or blocking the abuser offers sufficient protection (Afrouz and Vassos, 2024). Thus, understanding how anonymity exacerbates risks can enhance girls' awareness of potentially harmful online interactions, encouraging them to recognise unsafe behaviours early.

2.2. Understanding cyber violence through young people's voices

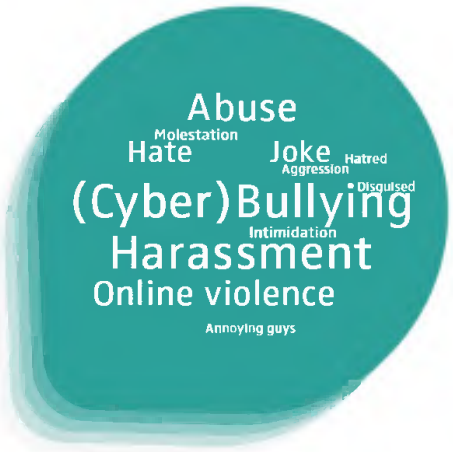
Insights from the focus groups with girls (aged 13-18), carried out within the framework of this study, provide a deeper understanding of these patterns. Girls demonstrated a multifaceted understanding of cyber violence, shaped by their lived experiences and social

environments. When asked about the term *cyber violence* ([25]), girls described a broad spectrum of everyday behaviours, rather than isolated or extreme incidents. These included verbal and psychological abuse; sexualised forms of cyber violence; coercion, manipulation, and blackmail; and body shaming and appearance-related judgment.

Before analysing the specific themes in detail, it is important to highlight the broader forms of online aggression highlighted earlier - verbal harassment, social exclusion, and reputational harm - which were also prevalent in these discussions. Girls often linked cyber violence to wider patterns of bullying, intimidation, and social exclusion. While these behaviours may not always be overtly sexual or gendered, they nonetheless contribute to digital environments in which girls frequently feel unsafe, scrutinised, or unwelcome.

Though less frequent, other important themes that emerged and are highly relevant to how girls understand and perceive cyber violence affecting girls are linked to gossip groups among peers, the ridiculing of mistakes, the spread of false rumours, and group bullying, all of which reinforce a sense of vulnerability in online settings. Additionally, girls used terms such as 'patriarchy', 'sexism', and 'discrimination', indicating an awareness that cyber violence is not just interpersonal but rooted in broader societal norms, gender stereotypes and gender inequalities.

Figure 2: Main terms used by girls to describe cyber violence as general aggression and violence



Source: Author's elaboration based on focus group discussions

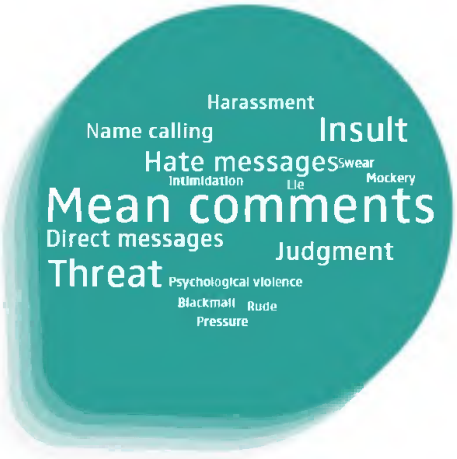
Girls also associated cyber violence with more generalised online aggression, including bullying and intimidation (Figure 2). Even when not explicitly sexual or gendered, such behaviours foster an environment of hostility in which girls feel unsafe, unwelcome, or under constant scrutiny.

Another recurring concern among girls is the misuse of technology to distort, manipulate, or steal personal content. Girls expressed fear over practices like photo editing, doxing, and the creation of

[25] This section offers a snapshot of how girls spontaneously interpreted and associated the term 'cyber violence' during the focus group discussions, in response to the question: 'What comes to mind when you hear the term cyber violence?' It reflects their initial, unfiltered perceptions and associations. The aim is not to redefine or develop a formal conceptual framework for cyber violence, nor to introduce new terminology. Instead, it sheds light on the language, images, and references that girls themselves use when thinking about the topic.

fake content using private images - highlighting a growing awareness that cyber violence often entails the loss of control over personal information and digital identity. In addition, girls identified behaviours such as stalking, invasion of privacy, the use of fake accounts, and anonymous calls as forms of cyber violence. This understanding, while not always linked to explicit threats, highlights a persistent sense of being monitored, watched, or tracked online.

Figure 3: Main terms used by girls to describe cyber violence as verbal and psychological abuse



Source: Author's elaboration based on focus group discussions

Verbal aggression online was described as especially pervasive, frequently occurring in comment sections, private messages, or group chats (Figure 3). Girls' testimonies reinforce research findings that online spaces are often defined by ambient hostility, where insults, threats, and harassment are experienced as routine rather than exceptional.

Figure 4: Main terms used by girls to describe cyber violence as sexual cyber violence

Source: Author's elaboration based on focus group discussions

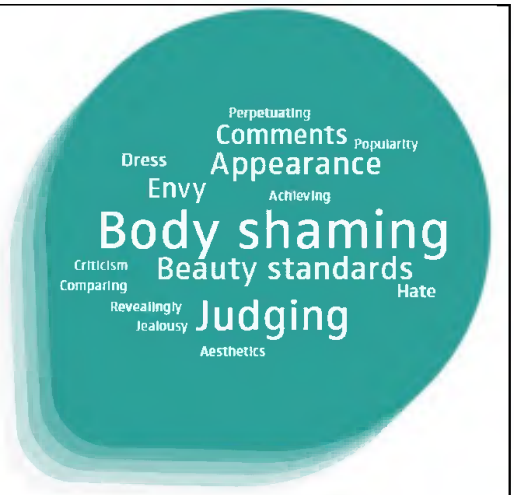
Sexual cyber violence emerged as a central concern for girls (Figure 4). They associated cyber violence with unsolicited nudes, grooming, image-based abuse, and revenge porn. Their language reflected a deep awareness of both the forms and emotional consequences of these behaviours.

Figure 5: Main terms used by girls to describe cyber violence as coercion, manipulation and blackmail

Source: Author's elaboration based on focus group discussions

Girls frequently pointed to manipulative methods as a significant aspect of cyber violence (Figure 5). Such methods - such as blackmail - were often framed as ongoing strategies of control that exploit trust and emotional vulnerability. One of the clearest manifestations of this dynamic is the pressure and coercion to share sexual content. Perpetrators exploit trust, manipulating victims into sending nude images or engaging in sexual interactions online. This pressure can escalate into blackmail, such as threats to leak private messages or images unless the victim complies (Salazar et al., 2023).

Figure 6: Main terms used by girls to describe cyber violence as body shaming, judgment and beauty standards



Source: Author's elaboration based on focus group discussions

Appearance-based judgment, body shaming, and social comparison were also cited as common and damaging forms of online harm (Figure 6), underscoring how gendered expectations and socially imposed beauty standards heighten girls' vulnerability to harm in digital environments.

As evidenced by literature in the field, girls' understanding of cyber violence also differed by age, reflecting their developmental stages, digital exposure, and social environments. Younger girls, aged 13 to 15, were more likely to focus on more immediate, visible, and relational forms of cyber violence. Their concerns were closely tied to familiar social settings such as school and peer groups. Many described experiences of bullying, exclusion from group chats, judgmental behaviour, and body shaming as key forms of online harm. They also expressed anxiety around appearance and

social comparison, frequently referencing beauty standards and body evaluation. A strong theme among this age group was fear of visibility and reputational damage, with terms like 'public humiliation', 'sharing screenshots', and sexually derogatory labels reflecting concerns about being exposed, judged, or ridiculed in online spaces.

Older girls aged 16 to 18 demonstrated a broader and more complex understanding of cyber violence, one that incorporated structural and psychological dimensions. They more frequently referenced sexualised forms of harm, including sextortion, revenge porn, coercion, and grooming, indicating a deeper awareness of emotional manipulation and sexual exploitation online. Mental health impacts were more commonly discussed in this group, with references to trauma, suicide, and long-term emotional harm reflecting a keen awareness of the enduring psychological consequences of cyber violence.

> 'Beauty standards are making it difficult for girls to feel like themselves and feel good with themselves … about how our body should look or our face or our hair. And I think that's why we see more bullying and violence towards the females.' (Girl 13-15, Cyprus)

Additionally, older girls appeared more familiar with technological misuse, describing incidents involving deepfakes and deepnudes, edited photos, and doxing, and expressing concern over the manipulation and theft of personal digital content. Their fears were heightened by the rapid advancement of AI, which they saw as enabling new and more harmful forms of cyber violence. One of the most alarming developments in this area is the proliferation of deepnudes or non-consensual synthetic intimate imagery videos (De Vido, 2024). The combination of readily available data, current technological capacity, and the spread of deepfake applications allows explicit videos to be fabricated without consent (EIGE, 2022a). This technological ease dramatically expands the potential pool of perpetrators and intensifies the risk, as harmful content can be generated and disseminated faster, more widely, and with greater anonymity than ever before.

Boys aged 15-18 years, on the other hand, demonstrated a multifaceted understanding of cyber violence as it affects girls, identifying behaviours that ranged from verbal harassment to more severe forms of sexual and psychological abuse. Bullying and verbal abuse - such as insults, threats, and swearing - were the most frequently cited forms of cyber violence among boys in this age group. These behaviours were commonly described as occurring within peer settings and were sometimes normalised or downplayed as part of everyday online culture.

> 'Now with AI I heard about a girl committing suicide because the boys from her class took pictures of her and thanks to AI, they made it look like she was naked and sent it to everyone'. (Girl 16-18, Poland)

Older boys more frequently identified sexual forms of cyber violence, including sextortion, non-consensual image sharing, and grooming. This suggests that awareness or exposure to such behaviours increases with age, though national and cultural contexts may also play a role. Indeed, in Cyprus, Romania and Ireland – the three countries where focus groups with boys were conducted - recent legislation has criminalised various forms of cyber violence. These legal changes seem to reinforce boys' awareness, not only broadening their understanding of the issue but also strengthening recognition of the serious emotional and reputational harm such actions can cause girls, particularly in cases involving the sharing of personal images or online blackmail.

Finally, boys also pointed to specific digital platforms where these behaviours occur, such as Fortnite and Snapchat. They described tactics like catfishing and the creation of fake accounts used to exploit, deceive, or humiliate others online.

3. How girls experience cyber violence

Focus group discussions with girls from all participating countries revealed a broad spectrum of experiences with cyber violence, both as victims and as witnesses, which we then categorised according to the forms in the Directive to avoid introducing new terms and concepts and to align more closely with those provided therein. These accounts point to four distinct yet interconnected forms of abuse: (sexual) cyber harassment, cyberstalking, cyber bullying and image-based cyber violence ([26]). These forms correspond to the literature's descriptions of verbal, psychological, and sexual abuse, as well as coercion and reputational attacks commonly encountered in girls' online lives. Participants consistently described digital spaces as hostile and unsafe. Many spoke openly about personal experiences of abuse, while others described incidents affecting peers.

(Sexual) cyber harassment

Sexual violence and exploitation emerged as the most frequently cited forms of cyber violence across countries and age groups. Participants reported receiving unsolicited sexual content and being confronted with predatory behaviour online. Examples included receiving explicit sexual images via Snapchat and encountering men on platforms such as Omegle ([27]) who would abruptly expose themselves during casual conversations. Participants also mentioned being added by accounts with sexually explicit usernames such as 'Horny in [name of the city]' ([28]) or 'sending nudes', which they described as a normalised and routine part of their online interactions.

Some participants recounted harassment by older men who would dismiss their age as irrelevant as *'it's okay, I don't mind'* when the girl disclosed being underage. Others described persistent targeting despite repeated blocking, with perpetrators creating multiple fake accounts to continue contact.

> 'There was this person who, from his profile, seemed to be an older man who sent messages because this girl had an Instagram profile and he kept sending her various provocative messages, asking her to send him photos of herself in her underwear or even without, perhaps in certain positions, not the most appropriate. And every time she blocked him, he created other profiles and continued to write to her, so he didn't accept rejection'. (Girl 13-15, Italy)

---

[26] See Table A.5 in Annex for specific examples of the types of cyber violence experienced by girls as victims and witnesses.
[27] Omegle, a free online chat platform that connected users anonymously, was shut down in November 2023. The platform faced increasing scrutiny over its role in facilitating harmful interactions, including sexual exploitation and abuse. Source: https://www.bbc.com/news/business-67364634
[28] The name of the city has been removed to protect the privacy and anonymity of the participants.

Cyberstalking and coercion

Cyberstalking and coercion were also common themes, with girls describing unwanted and persistent online contact. In Sweden, participants reported that photo requests often appeared early in conversations and escalated to pressure. In Italy, girls described older men circumventing blocks with fake profiles, and cases of emotional blackmail, such as ex-partners threatening suicide to manipulate girls into continued contact.

Some participants described coercion involving disturbing tactics, such as sending images of self-harm to compel compliance.

Cyber harassment (including cyberbullying)

Participants described cyberbullying and social exclusion as deliberate efforts to isolate, shame, or humiliate victims, often through peer networks. This included exclusion from group chats, targeted gossip, and the creation of online groups to ridicule specific individuals. Anonymous messaging on platforms like Instagram and TikTok was cited as a common vector for abuse.

> 'I think we've all noticed, either on TikTok or Instagram, a girl who posted photos and now there are messages … which are anonymous, and the things people write to her in those messages are very nasty and have very disgusting content'. (Girl 16-18, Cyprus)

Image-based cyber violence

The non-consensual creation, sharing, or manipulation of intimate images was reported as a widespread and a particularly damaging form of cyber violence. Participants described incidents involving deepnudes/ non-consensual synthetic intimate imagery, the secret recording during intimate moments, and image-based blackmail - even among younger age groups.

> 'She didn't want to date him, be in a relationship and he literally made a deepfake of her, and he started just sending it around school'. (Girl 13-15, Poland)

One girl discovered her ex-partner had secretly photographed her during intimate moments, leaving her terrified by the knowledge that the images could resurface.

> 'I was with a guy who I later found out had taken a picture of me when we had sex, it hasn't been shared but I'm still like this, he can keep it, he can keep it. It's unsafe to know that it's there, because even if he deleted it, he could still have it on his phone'. (Girl 13-15, Sweden)

Another recalled a case from primary school of image-based abuse and blackmail.

> 'I had a classmate in primary school… and someone took a picture of her, and it was really embarrassing, and he was threatening her that he would publish it if she didn't send him the homework or help him with the test and things like that, or money, even sometimes'. (Girl 13-15, Cyprus)

3.1. Where and how cyber violence happens: roles and interactions

Girls participating in the study described experiencing or witnessing cyber violence across a wide range of digital platforms (Figure 7). They stressed that abuse was not isolated to a single site or app; instead, it adapted to the technical features, cultures, and norms of each platform. In other words, the type of violence experienced was often shaped by what the platform enabled - whether anonymity, image-sharing, private messaging, or real-time interaction.

Figure 7: Forms of cyber violence associated with different digital platforms according to focus group participants

Platform	Description of the platform	Forms of violence
Instagram	Social media platform focused on photo and video sharing, including Stories and Reels.	Harassment via DMs; exposure of private photos; hate pages.
Snapchat	Multimedia messaging app known for disappearing messages, filters, and short-form video content	Unsolicited nudes; deepfakes; exposure accounts; suicide threats, offers of money for photos from unknown men.
TikTok	Social media platform centred on short-form video creation and sharing, popular for trends and music-based content	Grooming; sexist memes/comments; pornographic content in comments; 'sugar baby' solicitations*.
Discord	Communication platform designed for voice, video, and text chats, often used by gaming and interest-based communities	Grooming by adults; emotional manipulation; requests for nudes.
Omegle	Online chat website that randomly pairs users for anonymous text or video conversations	Repeated sexual flashing; coercive chat-based sexual interactions.
Gaming platforms (e.g., Valorant)	Interactive platforms where users play online multiplayer games, often with voice/text chat and competitive elements	Sexist voice chat abuse; constant belittlement of girls.
Messenger/ Chats	Instant messaging apps used for real-time text, voice, and video communication	Harassment groups; AI-generated content for mocking.
YouTube Kids	Video streaming app offering curated, age-appropriate content for children, with parental controls and educational content	Inappropriate content disguised as child-friendly videos.

*Sugar baby solicitations refer to situations where individuals - often adult men - approach younger girls or women with offers of financial or material support in exchange for attention, or sexual favours.

Source: Author's elaboration based on focus group discussions

Platforms such as Instagram, TikTok, Snapchat, and WhatsApp were highlighted as primary spaces where cyber violence occurs, ranging from harassment and bullying to verbal abuse and the non-consensual sharing of intimate images. Participants also noted that each platform's design shapes the risks they faced, such as TikTok's public comment sections, Snapchat's disappearing messages and WhatsApp group chats used for gossip or exclusion.

Even platform features such as emojis, fake accounts, and comment functions were understood as tools that could be used for bullying and harassment. Girls also expressed concern over algorithm-driven risks, particularly the rise of AI-generated deepfakes and manipulated content that reinforced sexist and violent norms.

On Instagram, girls reported receiving harassing messages through direct messaging (DMs), being targeted on hate pages, and having private photos shared without consent. Snapchat was described as a space where unsolicited nudes and deepfake images circulated widely, sometimes through exposure accounts ([29]). Some participants also recounted being pressured with threats of self-harm by perpetrators - such as by committing suicide - as a form of pressure or manipulation linked to image-based abuse.

TikTok was associated with a culture of normalised sexism. Grooming behaviours, body-shaming memes, and sexualised trends were cited as common, alongside comments that objectified or humiliated girls. Some girls described encountering solicitations for 'sugar baby/daddy' arrangements, suggesting that commercial forms of sexual exploitation were reaching younger audiences through the platform. Concerns were also raised about the lack of strict regulations on some social media platforms.

On other platforms, such as Discord, girls described being emotionally manipulated by older users, including cases of grooming and persistent pressure to send nudes. The platform's private and group chat features were seen as enabling prolonged, coercive interactions, often under the guise of shared gaming interests or community membership. Moreover, Omegle was described as a space of constant sexual exposure. Girls recounted being flashed or coerced into inappropriate chat exchanges by strangers, often adults.

> 'I was on this Omegle already with my friends on a sleepover… I connected with a guy like that. I'm like 'hey', 'where are you from', a conversation, and suddenly I'm 'wait, what are you doing?'… he put out his [genitals]. It's all the time!' (Girl 13-15, Poland)

Other private messaging apps such as Messenger were also described as hosting harassment, with participants describing group chats that exist solely to target girls, as well as the circulation of AI-generated content designed to mock or intimidate. Even platforms designed specifically for children were not exempt. On YouTube Kids, girls described

---

[29] Exposure accounts are social media profiles - often anonymous or unofficial - that are created and used specifically to publicly share personal, private, or sensitive content about individuals, typically without their consent.

encountering inappropriate or sexualised videos disguised as child-friendly, exposing them to harmful content at a very young age.

Online gaming environments, meanwhile, exposed girls to explicit sexism in voice chats. Girls described being told to *'go back to the kitchen'* or being belittled regardless of their gaming performance. Such experiences illustrate how gendered hostility remains deeply embedded in gaming culture.

Profiles of and relationship to perpetrators

Unlike offline forms of GBV, CVAWG has the potential to involve a wider and more diverse array of perpetrators. This is largely due to the ease with which individuals can participate in online abuse and amplify its harmful effects (UN Women, 2024b). In this context, two main types of perpetrators can be identified: primary perpetrators and secondary perpetrators (UN Women, 2024b). Primary perpetrators are those who initiate and incite incidents of online GBV. They are responsible for starting the harmful actions or content, whether through harassment, threats, or explicit violence. Secondary perpetrators, on the other hand, are individuals who contribute to the spread of CVAWG by downloading, forwarding, or sharing abusive content, thereby amplifying its reach and impact.

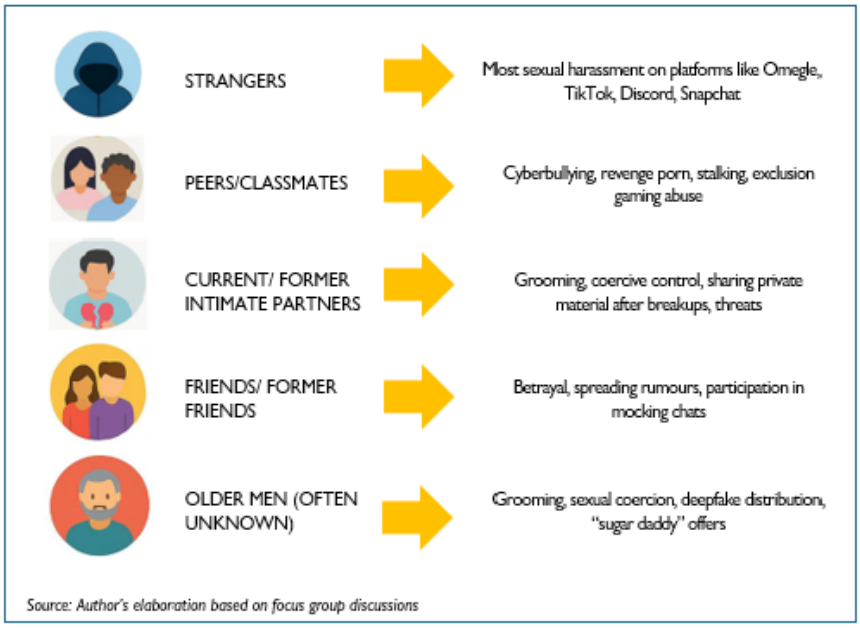
The European Women's Lobby (EWL) proposes a list of different types of online abusers ([30]). Perpetrators can be strangers to the victim, or they can be individuals from the victim's personal or professional circles, such as family members, friends, or colleagues. A global meta-analysis concerning offenders of online crimes against children provides estimations that, overall, 68% of all perpetrators were family members or acquaintances of the victim. Furthermore, 44% of perpetrators were under 18, suggesting a large proportion of peer-to-peer violence (Sutton and Finkelhor, 2023). More dangerous and organised groups, such as sexual predators, traffickers, paedophilic networks, and transnational criminal organisations, are also among the most significant categories of perpetrators in CVAWG cases (European Women's Lobby, 2017).

While acts of cyber violence occur online, the underlying motivations for these actions stem from the offline world, influenced by emotional, psychological, ideological and cultural factors that shape the perpetrator's profile and behaviour (Cybersafe project, 2020). Many young people (aged 12 - 18) often perceive perpetrators as victims themselves, describing them as lonely, weak, or also experiencing violence themselves. Family and relational dynamics - including parental monitoring, supervision, and family conflict and support - also play a significant role in shaping perpetration among youth (López-Castro and Priegue, 2019).

([30]) See Table A.8 in annex.

Focus group discussions across participating countries illustrate how these dynamics are experienced in practice.

Figure 8: Perpetrators and associated forms of cyber violence, according to focus group participants



Source: Author's elaboration based on focus group discussions

During the focus groups, girls consistently emphasised that cyber violence frequently originates **within their social circles or intimate relationships.** Cyberbullying and social exclusion typically involved classmates or peers, mirroring HBSC findings on peer perpetration, according to which cyberbullying perpetration peaks at age 13 for both boys and girls across most EU countries and regions ([31]). Within the context of peer groups, peer norms and attitudes heavily influence actions. Power, popularity, status and perceived notions of masculinity emerge as possible motivations for online harmful behaviours (DeSHAME Project, 2017).

Intimate relationships also emerged as a central context: girls described experiences of image-based abuse, coercion, and cyberstalking by romantic partners or former partners. Such cases illustrate how perpetrators exploit trust and intimacy to gain access to private material or to exert ongoing control.

([31]) See Figure A.13 and Figure A.14 in Annex.

> The person you are in a relationship with has a behaviour that you as a person do not like, you break up with that person, and they continue to write and to bombard you with messages. They do not accept this is over and continue to harass you. Or victimize himself and try to manipulate you to stay within the relationship. (Girl 16-18, Romania)

3.2. The pervasive and normalised nature of cyber violence

Girls consistently described cyber violence as pervasive and inescapable, aligning with research that demonstrates their disproportionate exposure to online abuse. Rather than viewing cyber violence as isolated incidents, girls described it as a pervasive and routine aspect of their digital lives. Many girls stated that almost every girl they knew had experienced some form of online abuse. Comment sections, group chats, and direct messages were described as unsafe spaces where hate, mockery, and judgment were commonplace. The anonymity of online spaces was frequently mentioned as a factor that emboldens perpetrators and allows harmful behaviour to occur without consequences.

The focus group findings also revealed a shared understanding that girls are more frequently targeted by cyber violence than boys. Girls described sexualised harassment, appearance-based insults, image-based abuse, and social exclusion as particularly gendered forms of abuse. While girls acknowledged that other girls can also perpetrate harm - especially through exclusion, mockery, or judgment - they were clear that boys were more often responsible for severe forms of abuse, such as coercing or sharing intimate images.

How peers respond to these incidents further compounds the harm. Victim-blaming plays a key role in how young people respond to these forms of abuse. Girls fear being blamed for sending intimate images or videos, for example, which can prevent them from seeking help or reporting the abuse. This fear of judgment can be exacerbated by psychological factors such as self-blame, reputational concerns, and shame (Mclocklin et al., 2024).

Online/Offline intersection of cyber violence

Cyber violence rarely remains confined to digital spaces. Girls described a blurring of boundaries between the online and offline worlds, where harassment, threats, and reputational damage originating on the internet frequently escalated into real-life situations or vice-versa. In this regard, existing research suggests that, for children, experiences of cyber violence are often closely linked to offline bullying, especially within school settings (Chiang et al., 2021).

This overlap between digital and physical spaces was also evident in the girls' accounts, which portrayed cyber violence as a continuum that seamlessly shifts between platforms, relationships, and environments. They often shared examples of online abuse leading directly to offline harm such as digital monitoring escalating into physical stalking.

'I know someone who was going out in a group of friends and a friend of her boyfriend kept writing to her. And when she said, I'm not interested in being more than friends, he kept insisting. And she said I will block you and never speak to me again. And the guy actually came to throw stones in her window at night'. (Girl 16-18 - Romania)

They also described how offline violence shifts into online spaces. Girls described situations where perpetrators, after engaging in face-to-face bullying or violence, continued harassment through social media or messaging platforms.

'…And then she decided to start posting videos on TikTok… some people from her school found her and wrote negative comments all the time, and it went viral and everyone started making fun of her'. (Girl 13-15, Cyprus)

In other cases, initial online interactions laid the groundwork for offline harm, such as prolonged harassment and stalking.

'Everything was fine for a few months, but then my friend had a lot of problems and had to go to counselling and see a psychiatrist because this guy would do anything to get her back, stalking her, sending her messages, and trying to deprive her of everything'. (Girl 16-18, Italy)

Another way the digital and offline overlap is evident in cases of emotional manipulation, where online abuse extended into victims' daily lives and disrupted their routines.

'…because he used to say to me that 'well if you don't write back to me, am I going to kill myself' and it was like he was, he was in a different time zone, so it often happened that I would stay up all night to talk to him, because I didn't want him to kill himself'. (Girl 13-15, Poland)

These accounts illustrate that young people do not experience online and offline life as distinct but as interconnected spaces, where online and offline forms of violence are deeply intertwined.

3.3. Young people's perspectives on intersectional risks in cyber violence

Qualitative insights drawn from the focus groups reveal the everyday realities of cyber violence and the social contexts shaping these experiences. Conversations with both girls

and boys highlighted how individual identity factors, together with broader social, structural, and cultural dynamics, contribute significantly to shaping their exposure to and experiences of online abuse. These lived experiences echo the findings of existing literature, which show that age, gender, and other intersecting social vulnerabilities play an important role girls experiences of cyber violence.

Individual/identity-based factors

Focus group participants demonstrated a strong and nuanced understanding of how personal characteristics - such as race, gender, disability, appearance, religion, and age - interact with social expectations and norms to increase their risk of exposure to online abuse.

Many described how online spaces replicate offline sexism, reinforcing patriarchal systems that undervalue and objectify women and girls. Posting personal content, especially images showing the body or those that do not conform to conventional beauty standards, was frequently linked to a heightened risk of receiving negative or sexualised comments. However, according to girls, simply being visible or active on social platforms often invites unwanted attention and criticism.

For example, girls who do not meet traditional standards of attractiveness or who physically stand out were perceived as more likely targets of shaming and objectification online. Several girls noted that those who *'stand out from the norm are more likely to get hate'.* In this context, beauty standards perpetuated online - often privileging thinness and a 'white' skin - lead to stigmatisation and bullying of those who do not conform (Azzarito et al., 2017).

'Women are not a minority, but they are still discriminated against for various reasons, and this is reflected online'. (Girl 16-18, Italy)

'I have friends… who have, for example, pictures in swimsuits. And all it takes is one such photo, and I have the impression that men feel that they are allowed to write'. (Girl 16–18, Poland)

Younger girls, especially in early adolescence, were seen as particularly at risk due to limited experience, lower digital literacy, and greater susceptibility to peer influence or grooming.

Girls also highlighted how discrimination based on identity - such as LGBTQ+ status - exacerbates risk. For example, one participant highlighted that transgender individuals, particularly trans women, often face delegitimisation and exclusion.

'Transgender people are often treated differently… told 'you're not a real woman'. (Girl 16-18, Germany)

This observation is supported by research showing that gender minorities within LGBTQ+ communities often face stigmatisation and harassment, with cyber violence intersecting with racist, anti-LGBTQ+, and transphobic abuse (Gius, 2023). Gender minorities report higher rates of online harassment, threats, and sexual harassment (Gamez-Guadix et al., 2022; Vogler et al., 2023). More specifically, non-binary, genderqueer, and transgender individuals encounter distinct risks and challenges compared to other minorities, underscoring the importance of more focused investigation in this area (Ray, 2024).

Disability was also noted as a significant factor increasing vulnerability. Girls shared that disabilities are often mocked through memes ([32]) or dehumanising humour, and people with disabilities are frequently pitied or devalued online. This echoes the FRA (2014) finding that women with disabilities experience higher rates of online threats and abuse.

Racism was another prominent issue raised by focus group participants, particularly against those that may belong to a racial or ethnic minority in their community or country. Religion was also referenced as a basis for online hate directed at girls, particularly those who visibly express their faith.

> 'I'm thinking specifically about people wearing the veil. They get a lot of hate online, it's very common'. (Girl 13-15, Sweden)

These insights underscore that exposure to cyber violence is determined not only by individual behaviour, but also by the intersection of identity, visibility, and entrenched social hierarchies.

Boys, on the other hand, pointed to individual traits and social positioning as factors that increase girls' exposure to cyber violence, suggesting that differences in appearance, personality, beliefs, or social status made them more likely targets. They interpreted girls' online behaviours - particularly sharing content perceived as provocative - as attention-seeking or driven by a psychological need for validation. Meanwhile, perpetrators were commonly viewed as socially marginalised *'losers'*, acting out of boredom, revenge, or a desire to assert dominance. This complements research showing that peer dynamics, social marginalisation, and power imbalances are key drivers of cyberbullying and harassment (Baas et al., 2013; Project deSHAME, 2017).

Boys' explanations of cyber violence affecting girls reflected an awareness of cultural norms, patriarchal attitudes, and gender stereotypes. Many acknowledged that societal figures and public discourse promote misogyny, creating a culture that normalises male dominance and shifts responsibility on girls, particularly in cases of image-based online abuse. However,

---

[32] A meme is an image, video, piece of text, or other type of content - typically humorous - that is copied and shared rapidly online, often with slight variations. In this context, focus group participants referred to memes created from images of individuals (often taken without consent or from private content), which are edited, captioned, or altered to mock, ridicule, or harass the person, and then circulated widely on the internet.

many expressed victim-blaming attitudes, with some boys holding girls accountable for abuse, especially when they posted *'provocative photos'*. However, a minority rejected victim-blaming, recognising that perpetrators bear responsibility. Boys' explanations and justifications reinforce the literature on normalisation and double standards, where male perpetrators are often excused while female victims are blamed, highlighting systemic gendered power imbalances (EIGE, 2025).

> 'Some girls post provocative photos of themselves online, and someone might grab them and do whatever they want with them and then comes the blackmail and everything else we mentioned earlier'. (Boy 15-18, Cyprus)

Boys also perceived girls as *'easier targets'* due to assumptions about emotional sensitivity or naivety, while less socially visible girls were seen as less at risk, linking exposure to visibility and social participation.

Gender norms and stereotypes further shape how boys experience and respond to cyber violence. Fear of social exclusion discouraged boys from speaking out, especially when bullied by girls, and parental reactions often reinforced expectations of toughness:

> 'They'll say, 'You're a man and you care what they say about you?'
>
> 'Like, if you tell your dad, 'He hit me', he'll just say, 'Hit him back'. That's how it is!'
> (Boys 15-18, Cyprus)

Social, structural, and cultural factors

Beyond individual traits, many girls pointed to wider structural and cultural factors that foster a permissive environment for cyber violence. They stressed that this violence is not the result of isolated online actions, but deeply rooted in social norms that blame girls for abuse while excusing or rewarding boys who perpetrate it.

Gender and cultural norms

Across all focus groups, boys highlighted how dominant norms of masculinity shape boys' online behaviour. A strong pattern emerged showing that boys often engage in cyber violence to gain validation and social approval from peers. Acts like non-consensual image sharing or group harassment are framed as performances to impress others or conform to peer expectations. In this context, girls are treated as *'trophies to show off to your friends'* and *'having had lots of girlfriends is seen as being an alpha male, a strong male'*. These peer-driven dynamics reflect the literature on adolescent risk-taking, social hierarchies, and exposure to sexualised interactions online (Project deSHAME, 2017).

Possessing or sharing intimate images is often treated by boys as a symbol of power and status, while girls involved are shamed. The logic of 'sexual conquest' and objectification was identified as a central driver of online abuse.

Younger girls, especially in Sweden, showed considerable awareness of male demand's role in online sexual exploitation, challenging victim-blaming narratives. This perspective aligns closely with Sweden's legal approach, which criminalises the purchase of sexual services.

Sexualisation and exploitation

Girls across countries linked cyber violence to wider systemic issues such as the pornography industry and early sexualisation of girls**.** Early exposure to pornography, especially when occurring in the context of limited age-appropriate comprehensive sexuality education, can shape boys' perceptions of women, often negatively. This supports evidence on systemic drivers of sexualised online abuse and adolescents' exposure to sexual content (Smahel et al., 2020).

> 'I think it's also very much down to the internet that women have become so easily accessible. The pornography alone… the fact that boys look at it at such an early age, that's really scary. And the fact that their view of women changes completely'. (Girl 13-

Normalisation and double standards

A recurring theme was the widespread minimisation or dismissal of boys' harmful online behaviours. Peers, adults, and institutions often excuse these actions as immaturity or jokes, contributing to a culture where such violence is normalised for men but remains a serious issue for women. Both girls and boys consistently described how girls who experience cyber violence are often judged, ridiculed, or held responsible for the abuse, while boys are excused - or in some cases even praised - for the same behaviours.

> 'When boys do it, it's like 'oh, they're just having a laugh'. (Girl 13-15, Ireland)

> 'If a boy shares a photo, he's considered cool. If a girl does it, she's done something wrong'. (Girl 16-18, Italy)

Several girls reflected on how some boys' aggression in online spaces may stem from insecurity, emotional immaturity, or fear of rejection. In these cases, cyber violence was perceived not only as a way to impress peers but also as a means to assert control or mask personal vulnerability. Others, however, described such actions as deliberate and malicious, particularly in situations involving breakups or perceived rejection.

Girls also highlighted the role of certain online subcultures and influencers in shaping misogynistic attitudes. Spaces such as *incel* forums ([33]) were described as echo chambers that channel men's frustration and sense of rejection into hostility towards women, reinforcing harmful stereotypes and legitimising abusive behaviour.

While many girls strongly rejected the notion that victims are responsible for their own abuse, a few expressed more ambivalent views. These participants stressed that although girls are not to blame, they should be aware of potential risks. Such perspectives illustrate the tension between rejecting victim-blaming narratives and recognising how social norms shape perceptions of 'risk' and responsibility.

Relationships as high-risk contexts

Finally, romantic and intimate relationships were repeatedly identified as high-risk contexts for cyber violence. Girls described experiences involving emotional manipulation, coercion into sharing intimate images, and betrayal of trust when those images were later shared or used for blackmail. This dynamic is exacerbated by the tendency of some young people to interpret controlling or aggressive online behaviours as signs of affection or attention, inadvertently normalising abuse (Lu et al., 2021). Such misinterpretations can delay help-seeking and contribute to underreporting.

> 'A lot also has to do with manipulation. How much the boy really wants something from her and how much he manages to get her under his claws and then really just works towards that and then just drops her afterwards'.
>
> 'I also think that in a relationship it gets worse or more difficult, because then you have these 'rose-coloured glasses' … and then this complete trust, which makes it more difficult to realise that it's not trust or that he doesn't deserve trust'. (Girls 16-18 – Germany)

Girls explained that trust and emotional dependency within relationships can make it hard for girls to resist coercion or recognise harmful behaviours. Violence in relationships was often seen as 'normal', difficult to identify (*'you're so blinded'*), or excusable. There is, indeed, a mixed understanding among young people about what constitutes acceptable behaviour in cyber-dating; some consider technology-facilitated intimate partner violence as a 'relationship issue' rather than as a form of violence. This echoes current debate on what is 'normal' and what is not ([34]).

([33]) Incel forums are online communities where individuals who identify as 'involuntary celibates' (incel) share frustrations about their perceived inability to form romantic or sexual relationships. These spaces often include content expressing resentment and, in some cases, hostile or misogynistic views.

([34]) For more info. please see: Tech-facilitated abuse and the 'new normal' - City Vision

Breakups were frequently identified as a critical flashpoint, often triggering acts of revenge such as non-consensual sharing of private and often intimate images, including AI-created imagery, ongoing harassment, or public shaming. These patterns underscore how online abuse is deeply tied to power, control, and the enforcement of gendered norms - even, and especially, within intimate relationships.

Perspectives from boys

Peer group dynamics emerged as a central driver of cyber violence. Boys explained that engaging in harassment can elevate one's social standing, particularly when high-status boys set the tone for abusive behaviour. This can foster a 'mob mentality' in which loyalty to the group is valued above individual relationships.

Masculinity norms and peer pressure were cited as consistent drivers of abuse. Online harassment - particularly mocking girls or sharing intimate images - was often framed as a way for boys to demonstrate toughness, prove masculinity, or gain peer approval. Opting out of such behaviour could be seen as *'less masculine'*, making participation a means to *'prove they're more manly'*.

These dynamics were further shaped by gendered double standards and underlying homophobia. Participants pointed out that identical behaviours - such as posting revealing photos - were judged differently depending on the person's gender. Girls were labelled provocative, whereas boys were mocked or ridiculed.

Some participants demonstrated awareness of broader systemic inequalities, but this recognition often coexisted with persistent victim-blaming attitudes:

> 'Well, you post a naked photo online and expect a different response from people?' (Boy 15-18, Cyprus)

Overall, the discussions revealed how deeply entrenched gender norms, double standards, and power imbalances sustain a culture where cyber violence is normalised and responsibility is frequently shifted onto girls, and perpetrators face little accountability.

3.4. Role of bystanders and peer influence

Bystanders play a crucial role in reducing the impact of cyber violence on victims. Intervening is recognised as a key strategy to combat this type of violence and mitigate its harmful effects. Offering direct support, such as comforting victims, can help reduce the emotional harm they experience. Indirect support, like reporting incidents to authorities, can reduce the prevalence of harmful content online and promote positive actions among internet users (Rudnicki et al., 2023).

Despite this potential, many bystanders remain passive when encountering online hate. Research on cyberbullying reveals that approximately 50-90% of adolescents had, at some stage, been a passive bystander to cyberbullying, failing to intervene in response to this type of abuse (Allison and Bussey, 2016). Moreover, bystanders are more likely to act if they feel a connection to the victim and perceive the situation as safe, ensuring they will not become targets themselves. Without these conditions, bystanders are less likely to take action and may even contribute to the spread of cyber violence.

Dominguez-Hernandez et al. (2018) identified a range of factors that influence whether young bystanders under the age of 20 choose to intervene in cyberbullying situations ([35]). These include contextual factors (e.g., friendships, social norms, incident severity, fear of retaliation, and bystander dynamics) and personal factors (e.g., empathy, moral disengagement, self-efficacy, and past experience). Similar themes emerged in the focus groups with boys, who expressed complex attitudes, dilemmas, and justifications about their roles as bystanders to cyber violence against girls. Three recurring patterns were evident: passive bystanding and avoidance as a form of self-preservation, peer norms that discouraged intervention, and limited confidence in the effectiveness of taking action.

Passive bystanding and avoidance

Many boys described themselves as passive observers, often choosing to 'just watch' or record incidents rather than intervene - especially when the victim is a stranger. Fear of retaliation or of escalating the situation also influenced avoidance.

Boys often expressed the belief that victims should resolve issues themselves, particularly if they were not close friends. Such responses suggest a tendency to frame cyber violence as a personal issue rather than a collective responsibility, reinforcing patterns of victim-blaming. Peer pressure and group dynamics also strongly shaped bystander behaviour. Many participants feared social exclusion or ridicule if they acted against the group. Some boys reported offering discreet support - such as private messages - rather than public intervention.

> 'If you saw all your classmates just like seeing this and not doing anything, you wouldn't want to be the odd one out'. (Boy 15-18, Ireland)

Low faith in bystander intervention

Overall, boys expressed scepticism about the effectiveness of intervening to stop cyber violence against girls. Many felt that taking a stand would expose them to criticism. Others emphasised lack of motivation when they did not personally know the victim. These findings find echo in the existing literature on bystander behaviour and masculinities in

---

([35]) The key findings from their study are summarised in Table A.9 in annex.

online settings. Research shows that male peer groups often discourage intervention when witnessing online abuse because taking a stand can threaten one's social status or masculine identity (De Keseredy and Schwartz, 2013; Connell, 2005). Studies on cyber violence further suggest that digital environments amplify these social risks: intervening against sexist or aggressive content can expose boys to ridicule or retaliation from peers (Powell and Henry, 2017). Moreover, empirical evidence indicates that empathy and personal connection to the victim are crucial motivators for bystander action - when these are absent, the likelihood of intervention in cyberbullying or online harassment decreases significantly (Barlińska et al., 2013). Together, these studies highlight how peer norms, fear of social repercussions, and emotional distance shape boys' reluctance to intervene in instances of cyber violence against girls.

'Miss, I've got my own problems, I'm not going to sit and deal with other people's issues'. (Boy 15-18, Cyprus)

Several boys also believe that simple appeals to peers to stop their behaviour are ineffective, as *'people aren't going to listen if you just say, oh, stop or whatever. Words aren't going to do much'*. However, some participants recognised that peer influence - especially from a male friend or older brother - could be effective in discouraging harmful behaviour, particularly at an early stage.

Some boys also acknowledged the potential value of reaching out to victims privately. While such actions show empathy, they also reflect a reluctance to challenge harmful behaviours publicly.

4. Effects of cyber violence

4.1. Impacts of cyber violence and social dynamics

While cyber violence can impact anyone, women and girls are disproportionately affected, often enduring more severe and traumatic forms that result in long-lasting effects on their behaviour, emotions, mental health, physical well-being, and social interactions. Such consequences are no different from those of offline harassment, bullying, and stalking, but with stronger negative impacts (European Women's Lobby, 2017).

For girls and young women, the psychological impacts of CVAWG are particularly severe. Adolescents targeted by cyberbullying frequently report depression, anxiety, and tendencies toward self-harm (Nixon, 2014). Younger victims often report feelings of sadness, hopelessness, anger, and fear, with some studies suggesting that cyberbullying may be even more stressful than traditional bullying due to the anonymity of perpetrators and the pervasive reach of online platforms (Sourander et al., 2010).

Different forms of cyber violence result in varying levels of harm, with visual content like pictures and videos causing the most severe psychological effects (Nixon, 2014). Cyberbullying also disrupts social relationships, contributing to isolation, diminished trust, loneliness, and reduced self-esteem (Sciacca et al., 2023). These challenges are exacerbated by victims' reluctance to report or seek help, driven by fear of judgment, uncertainty about outcomes, and doubts about how adults might respond (Project deSHAME, 2017). Indeed, whether young seek help or try to handle things on their own depends on several factors: whether they recognise the behaviour as abusive, whether they know about available support, and whether they believe that family, schools, or digital platforms can actually help. In practice, many youths only reach out after the abuse has caused significant harm - emotional, reputational, physical, or financial (Freed et al., 2025). Other studies, thus, underline the need of tools and policies to mitigate the harm of cyber violence and improve help-seeking (Janickyj and Tanczer, 2025).

European data confirms the effect on wellbeing by the heightened exposure of girls and young women to online harm compared to boys and young men. As shown in Figure A.11 in Annex, in all EU represented countries except Lithuania, a significantly higher proportion of girls report harm [36] – with an average gender difference of 19 percentage points. Age patterns show less consistency (see Figure A.12 in Annex). In countries such as Poland, Malta, and Lithuania, older children report higher levels of harm, while in others, like Czechia, Estonia, Portugal, Romania, and Slovakia, younger children are more affected.

[36] In the context of this project, 'harm ' refers to the level of distress or upset experienced by the surveyed child or teen.

4.2. Youth voices on the consequences of cyber violence

Focus group discussions with girls confirmed these trends. Girls described the impact of cyber violence using emotionally charged terms such as 'depression', 'suicide', and 'trauma', reflecting their awareness not only of immediate harms but also of long-term emotional consequences. Boys echoed these understandings, recognising the sadness, insecurity, and desperation victims often feel. The fear of reputational damage emerged as particularly acute for girls and young women, who are frequently judged more harshly than boys in similar situations (Project deSHAME, 2017).

Emotional and psychological distress

The most pervasive theme emerging from the focus groups was the emotional and psychological impact of cyber violence. Participants described cyber violence as not only harmful in the moment but also as having lasting effects on mental health and social interactions.

Girls frequently expressed feelings of sadness, fear, anxiety, insecurity, and worthlessness, especially when responding to harassment, bullying, or image-based abuse. Emotional distress was often compounded by self-blame and shame, which made seeking support or speaking out even more difficult.

> 'I know a girl that some people, mostly boys, were sending weird messages to her saying that they wanted to see her face and she actually sent people her face and everything and she was feeling really bad and started covering her face everywhere. This created a huge impact on her life and eventually led to her being depressed and she couldn't go to school'. (Girl 16-18, Cyprus)

Some girls shared stories of peers experiencing severe distress, including suicidal thoughts, self-harm, and depression, often following public exposure or online shaming. Appearance-based bullying, particularly regarding body weight or shape, was cited as especially harmful, fostering relentless scrutiny, often from anonymous perpetrators.

Loss of trust and social isolation

Another key consequence of cyber violence identified by participants was a loss of trust, particularly towards peers, intimate partners, and online communities. Victims often described emotional withdrawal and wariness towards future interactions.

Cyber violence can also lead to social isolation and peer rejection. One participant suggested that when private images are shared without consent, the victim is no longer seen as a full person, but is instead reduced to the content of those images. As a result, peers may actively withdraw, reinforcing exclusion.

'I think she'll probably be reduced to just that… and people will actually forget who she really is. But then it will really just be, these are the photos, that it's her body, not her anymore'. (Girl 16-18, Germany)

Digital exclusion

Cyber violence can restrict girls' participation in social and civic digital spaces. Harassment and sexist backlash often lead them to withdraw from online gaming, political debates, content creation, and other interactive spaces. In many cases, the threat of abuse was enough to silence their voices or deter them from engaging in online spaces. In some cases, victims resorted to uninstalling apps or even changing schools to escape harassment.

'If you want to start playing games, but you can't play games because you're met with sexist comments. If you just want to act in politics, but you are met with… threats sent simply on your social media. You want to act, but you are met with heckling. You want to run for campaign, but someone creates a trolling account for you ( ) … The question is whether it's worth it. So, for me it just boils down to such an attempt to exclude'. (Girl 16-18, Poland)

Normalisation of violence

A subtle yet significant impact identified by focus group participants was the normalisation of harmful behaviours. Many girls observed that frequent exposure to cyber violence can lead to desensitisation, reducing the perceived seriousness of certain forms of abuse, leading young generations to *'don't take them that seriously'.*

Several participants said they had grown up aware of both online and offline risks. They recalled being taught from an early age to be cautious. Despite this awareness, some girls expressed a sense of resignation, viewing cyber violence as inevitable and, therefore, with the need to adapt to this reality. This sentiment was voiced strongly in Belgium, where participants described cyberbullying as 'part of life' and nearly impossible to escape.

'Honestly, I don't think we can do much. The system is like that. To avoid it, you just have to blend in and disappear. Once it's over, it's over. It's a phase of life - you go through it and move on'. (Girl 13-15, Belgium)

The enduring nature of online abuse was another major source of fear and anxiety. Participants described how harmful content - such as private photos - can resurface at any time, creating a persistent sense of vulnerability and threat. They noted that the same image or message might reappear in a different group chat or context, leaving them feeling powerless to prevent re-exposure.

5. Preventing and addressing cyber violence

5.1. International and EU frameworks addressing CVAWG

While the EU does not have a standalone legal framework dedicated exclusively to gender-based cyber violence, recent progress includes the adoption of the aforementioned Directive (EU) 2024/1385 on combatting violence against women and domestic violence, which criminalises four main forms of cyber violence: the non-consensual sharing of intimate or manipulated materials, cyberstalking, cyber harassment (including cyber flashing ([37])), and cyber incitement to violence or hatred.

Set to be transposed by June 2027, this Directive marks a significant milestone in addressing cyber violence: it explicitly recognises cyber violence as a form of GBV and requires MS to adopt preventive measures, to develop accessible and secure ICT reporting channels, to take suitable measures to ensure takedown of the content related to the offence, to provide specialist victim support services, to facilitate access to justice, and coordination and cooperation between authorities. It also encourages Member States to ensure that their national procedures stay abreast of technological developments. This Directive marks a historic step as it requires all EU MS to criminalise various forms of cyber violence.

The evolution in EU policy reflects a growing awareness of the intersecting vulnerabilities experienced by women and girls, shaped by factors such as age, ethnicity, and socioeconomic status. Throughout the EU's broader regulatory landscape - including data protection, online content moderation, victim support mechanisms, and child protection strategies - Directive 2024/1385 serves as the central framework that connects these initiatives, harmonising measures across MS to criminalise and prevent cyber violence, protect victims, and promote accountability online. Thus, while EU legislation does not take the form of a single, unified framework on cyber violence, a combination of binding and non-binding mechanisms has emerged to address the issue comprehensively.

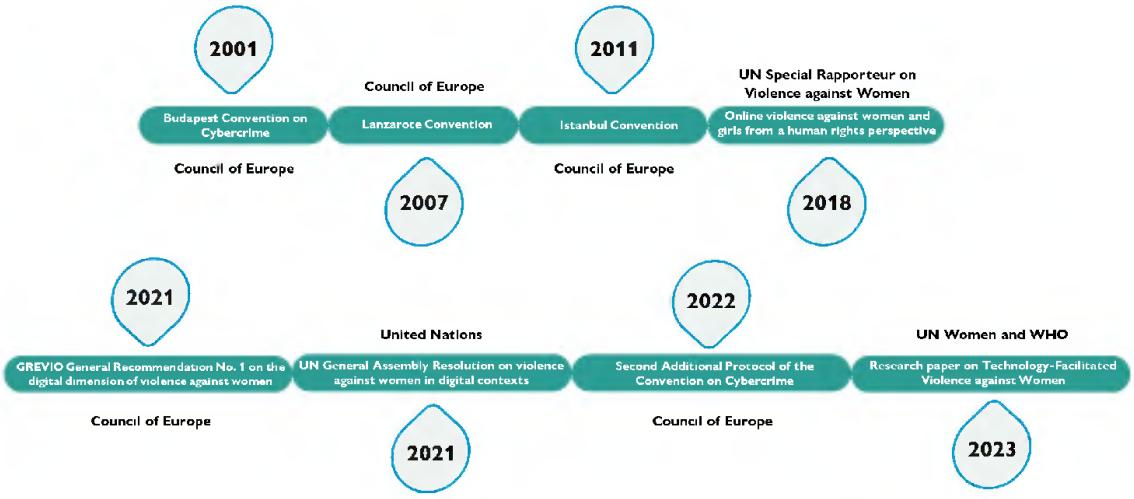
5.1.1. International frameworks addressing cyber violence

At the international level, several key instruments ([38]) provide standards and guidance that have shaped EU action. United Nations (UN) documents, including the 2021 UN General Assembly Resolution on violence against women in digital contexts, the 2018 report of the UN Special Rapporteur on Violence against Women, and UN Women and WHO's 2023 research paper on technology-facilitated violence against women, emphasise international

([37]) Cyberflashing is defined in the Directive as 'the unsolicited sending of an image, video or other similar material depicting genitals to a person (Article 24).
([38]) Please see Figure 9 below. Detailed descriptions of examples of international instruments are provided in Table A.1 in Annex.

cooperation, platform accountability, victim-centred remedies, and the inclusion of diverse perspectives in evidence collection and policymaking. The Council of Europe has advanced relevant frameworks such as the Istanbul Convention (2011), which explicitly addresses online abuse; the Budapest Convention on Cybercrime (2001) and its 2022 Second Additional Protocol, which enable cross-border cooperation in prosecuting cyber offences; and the Lanzarote Convention (2007), which protects children from sexual exploitation, including in digital spaces. In addition, GREVIO General Recommendation No. 1 on the digital dimension of violence against women (2021) highlights the importance of national action plans, digital literacy, and specialised training for law enforcement and judicial personnel on cyber violence. Together, these instruments provide guidance for prevention, policy development, and the provision of support services.

Figure 9: Timeline of examples of leading international legal and policy instruments addressing cyber violence



Source: Author's elaboration

In November 2025, the Council of Europe approved a Recommendation on accountability for technology-facilitated violence against women and girls ([39]).

([39]) Approval of key instrument on accountability for technology-facilitated violence against women and girls - Gender Equality

5.1.2. EU regulatory developments on gender-based cyber violence

The EU has progressively strengthened its regulatory framework to address gender-based cyber violence, drawing on a wide range of legal and policy instruments ([40]).

Adopted in 2018, the General Data Protection Regulation (GDPR) has strengthened individuals' rights over their personal data and has established safeguards against misuse. It has also provided for personal right to request of removal of harmful or non-consensual personal content online. While its privacy-based protection have been frequently used by victims of cyber violence, the effects of these provisions in successfully addressing gender-based forms of online abuse have been found limited (European Parliament, 2024).).). More recently, the Digital Services Act (DSA), and the Artificial Intelligence Act (2024/1689)) strengthen online safety by introducing stricter content moderation rules, enhanced victim protections, and transparency requirements in the use of AI, including deepfake technologies. These advances demonstrate growing recognition of the issue of cyber violence and the need for coordinated action across MS.

Victim protection measures are equally central. The Victims' Rights Directive (2012/29/EU), currently under revision, sets minimum standards for support services, while the EU Strategy on Victims' Rights (2020–2025) highlights the need for stronger protections in cases of cyber violence. Complementing this, the Gender Equality Strategy (2020–2025) explicitly calls for tackling online GBV.

Child protection instruments also play an important role. The Directive (EU) 2011/93 on combating the sexual abuse and sexual exploitation of children and child sexual abuse material, the primary legal instrument is under revision to reflect technological advances since its adoption in 2011 (EPRS, 2024). Regulation (EU) 2021/1232 enables providers to detect and block child sexual abuse material, while the EU Strategy for a more effective fight against child sexual abuse (2020–2025) and the Better Internet for Kids (BIK) Strategy strengthen online safety for children. The proposed EU Centre on Child Sexual Abuse further aims to centralise resources and improve victim assistance.

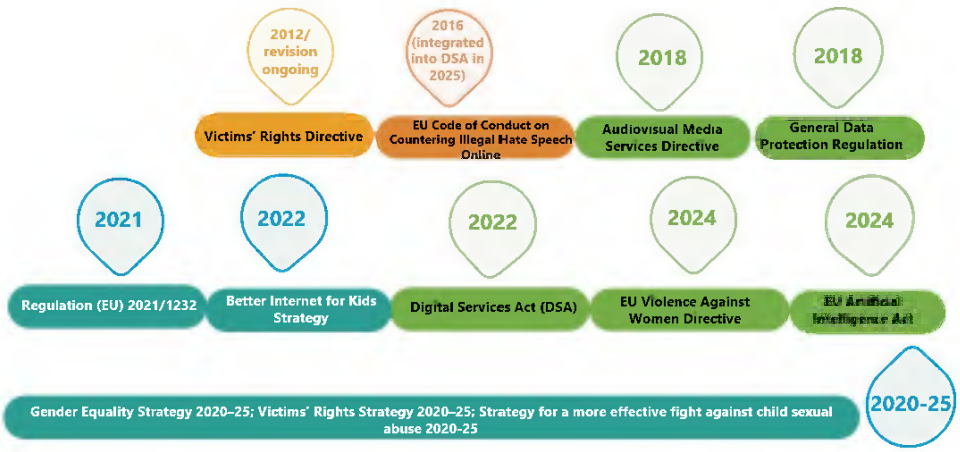
Alongside these frameworks, initiatives addressing hate speech play an important role. The 2016 EU Code of Conduct on Countering Illegal Hate Speech Online - recently integrated into the DSA (2025) - reinforces commitments by major platforms to address hate speech and adopt best practices. Similarly, the Audio-visual Media Services Directive (2018/1808) includes provisions against hate speech and enhances protections in online media environments.

The adoption of the Directive (EU) 2024/1385 on combating violence against women and domestic violence (the EU VAW/DV Directive) in 2024 constitutes the most recent and

significant legislative commitment to combating CVAWG. It requests Member States to criminalise cyber violence by setting minimum standards for criminalisation of the four main forms of cyber violence, including non-consensual sharing of intimate or manipulated material, cyber stalking, cyber harassment and cyber incitement to hatred or violence.

This leaves the possibility for Member States to develop stricter national rules and penalties. In doing so, the transposition of the Directive is likely to address some of the most persistent challenges in developing an EU-wide approach to tackling cyber violence namely the lack of harmonised definitions across countries and jurisdictions (EIGE, 2025 p66). Because it also requires Member States to collect data on these four forms of cyber-violence, thus paving the way towards comparable data across countries. To facilitate this process, EIGE was specifically tasked with establishing common standards and supporting Member States with the collection of comparable and standardised administrative data (EIGE, 2025).

Figure 10: timeline of examples of main EU regulatory developments on gender-based (cyber) violence as of December 2025*



* Main measures can be grouped into four categories:

	Expanding support systems for victims
	Monitoring and evaluation through collaboration
	Strengthening legal protections amid emerging challenges
	Measures to protect children and address gender-specific risks

Source: Author's elaboration

5.2. National approaches in EU Member States

Across the EU, national responses to GBV and to cyber violence vary considerably, reflecting different legal frameworks, cultural contexts, and technological capacities among

MS. In most MS, general criminal offences - such as harassment and stalking - are applied to both physical and digital forms of violence, including cyber harassment and cyberstalking. Legal precedents have extended these traditional definitions to online contexts. However, when cyber violence is addressed through such general offences, cyber violence often lacks gender-specific language and rarely makes explicit reference women.

While few countries have laws specifically targeting CVAWG, legislative efforts are underway in many MS to introduce tailored provisions. In most cases, national laws rely on general criminal offences like harassment and bullying, supplemented by broader definitions and civil protections.

5.2.1. Legal approaches across the EU

EU MS have adopted different legislative approaches to address cyber violence. These include enacting dedicated cyber violence laws, integrating cyber-specific offences into existing legislation, or embedding protection within broader frameworks on violence against women or privacy. Many countries combine these approaches, resulting in mixed legal systems.

The 2022 EIGE study on Combating Cyber Violence against Women and Girls (EIGE, 2022b) classifies national legal approaches into three categories: treating cyber violence as a distinct offence, as an aggravating factor, or as part of general offences. It also identifies national laws that explicitly mention women, girls, or children, and reviews national policies on cyber violence that include targeted protections for these groups.

Building on the study's findings, three main types of approaches can be identified, as it follows below. The analysis reveals a proactive shift among MS toward victim-centred approaches, cross-border cooperation, and the inclusion of digital safety in broader strategies against violence and cybercrime. In addition, Table A.3 in Annex provides detailed examples of national Case Law related to cyber violence.

Enacting specific cyber violence laws

Some countries such as Belgium, France, Denmark and Portugal have adopted standalone laws or provisions that directly criminalise different forms of cyber violence. These include measures against cyberbullying, school and university harassment, image-based sexual abuse, and the non-consensual sharing of intimate content. There has been the introduction of obligations for online platforms to remove harmful content, facilitate user reporting, and preserve digital evidence.

Table 1: Examples of specific cyber violence legislation at national level

Country	Name of the measure and year	Description
Belgium	Law aimed at combating the non-consensual distribution of sexually explicit images and recordings (4 May 2020)	The law extends the competency of the Institute for the Equality of Women and Men to take legal action and assist adult victims of digital sexual violence, including non-consensual distribution, sextortion and deepnudes. The IEWM provides advice and support in removing non-consensual images. To this end, it works together with internet platforms such as Meta, Google and Pornhub, the platform stopncii.org and the federal police. Another institution, Child Focus is responsible for underage victims.
France	Law No. 2020-766 aimed at combating hateful content online (Avia Law)	It required platforms to remove explicit illegal content (e.g. hate speech, child pornography) within 24 hours, with penalties for non-compliance. The Constitutional Council later declared key provisions of the law unconstitutional, citing concerns related to freedom of expression. However, the remaining provisions included the creation of a public prosecutor's office for online hate and an Online Hate Observatory within the *Autorité de regulation de la communication audiovisuelle et numérique (Arcom).*
	Law No. 2022-299 aimed at combating school bullying	It criminalises school/university bullying (incl. cyber), up to €150,000 fine and 10 years prison. It provides for the collection and preservation of digital evidence in relation to the cyber offence.
	Law No. 2023-566 aimed at establishing a digital majority and combating online hate speech	Platform obligations to facilitate reporting of content that infringes upon personal rights and to provide preventive information to users.
	Law No. 2024-449 on Securing and Regulating the Digital Space (SREN Act)	It regulates digital spaces, focusing on protecting citizens, particularly minors, from harmful content and combatting cyber harassment, sextortion, online scams, hate, and disinformation. The law introduces a new offence relating to sexual deepfakes, punishable by two years' imprisonment and a fine of 60,000 euros for disseminating a sexual deepfake publicly or to a third party without the person's consent. Sanctions increase to 3 years' imprisonment and 75,000 euros fine if published using an online public communication service. The law also imposes age verification systems on pornographic websites, under penalty of heavy fines and site blocking. This law entered into force in June 2025 and applies to all major pornographic websites.
Denmark	Penal Code Article 264d	It criminalises the non-consensual sharing of intimate images or videos, punishable by up to three years' imprisonment, with harsher penalties for cases involving minors or mass distribution.

Country	Name of the measure and year	Description
		Although gender-neutral, it targets abuse that disproportionately impacts women and girls.
	Penal Code Articles 225, 231 and 242	Section 225 criminalises sextortion, and Section 231 criminalises grooming and Section 242 criminalises stalking provision.
Portugal	Article 193 of the Penal Code / 2023	Law No. 26/2023 of 30 May amended the Penal Code by altering Article 193 to criminalise through media, the Internet or other means of widespread public dissemination. It provides that anyone who, without consent, disseminates or contributes to the dissemination of images, photographs or recordings that invade a person's private life, including the intimacy of family or sexual life, may be punished with imprisonment of up to five years, thereby strengthening legal protection against non-consensual sharing of intimate content online. The same law also amended Article 197 to provide aggravating circumstances, penalties for certain crimes increased by one-third if the offence is committed through social media, the Internet, or other widespread digital dissemination.

Expanding existing criminal codes to address cyber violence

Other jurisdictions have adapted pre-existing criminal provisions to cover online contexts. This is the case for countries such as Austria, Finland[41], Germany, Ireland, Italy, Poland, and Romania. Offences such as stalking, harassment, grooming, defamation, and hate speech have been extended to include digital environments. Amendments in this area often recognise cyber violence as part of gender-based violence or domestic violence, enabling courts to impose enhanced penalties and protective measures when cases involve intimate partners or minors. This approach provides legal continuity and consistency but can lead to ambiguities, as offences are not always explicitly defined as cyber-related, resulting in variable enforcement and limited gender sensitivity.

Table 2: Examples of national criminal code provisions related to cyber violence

Country	Name of the measure and year	Description
Austria	§107a StGB – Criminal Code	It criminalises cyberstalking.
	§107c StGB – Criminal Code	It targets persistent online harassment.

[41] In Finland, criminal provisions are neutral from a technological perspective, that is, their implementation does not depend on the means used e.g. in stalking.

	Hate on the Internet Act / 2021	The legislative package introduced measures to improve the legal situation of those affected by cyber violence. For example, it facilitates civil claims against online hate. Victims of cyber violence are granted injunctive relief for hate postings that violate their human dignity. Such postings must be removed immediately. Victims of online hate are also entitled to free psychosocial and legal assistance in court proceedings. The criminal offence of incitement to hatred/hate speech has been strengthened and the scope of the offence of cyberbullying has been extended. The offence of 'upskirting' has also been added to the Austrian Criminal Code.
Belgium	Article 417/8 and Article 417/9 of the Penal Code	The Belgian Penal Code criminalises the creation and distribution of deepnudes without consent. Creating a deepnude without the person's consent is considered a form of voyeurism (Article 417/8) and while distributing a deepnude constitutes the non-consensual distribution of content of a sexual nature (Article 417/9 of the Penal Code)
Finland	Criminal Code	While Finland relies on general criminal provisions, recent amendment of criminal code has expanded the application of sexual harassment law to include online contexts, providing better protection for victims of cyber violence. In particular, the law criminalises defamation, sexual harassment, illegal threat, stalking, violations of privacy, and hate speech. These offences are applicable regardless of whether they occur online or offline.
Germany	Network Enforcement Act (NetzDG) / 2017	It mandates rapid removal of illegal content [42], including hate speech, and requires platforms to publish compliance reports. It also includes child protection measures and provisions against disinformation.
	Section 176 of the Criminal Code (*Strafgesetzbuch* – StGB)	Expanded in 2020, it criminalises cyber-grooming, including attempted grooming.
	Reform of the Youth Protection Act (*Jugendschutzgesetz* - JuSchG) / 2021	It was reformed to enhance digital child protection [43].
Ireland	Harassment, Harmful Communications and Related Offences Act / 2020	Also known as 'Coco's Law', it criminalises online abuse such as the non-consensual sharing of intimate images and cyber harassment. Intimate partner relationships constitute an aggravating factor in sentencing.
Italy	Law Decree No. 11/2009	It introduced Article 612-bis on stalking in the criminal code.

[42] The law requires social media platforms with over 2 million users to remove 'clearly illegal' content within 24 hours and all illegal content within 7 days of its posting, with a maximum fine of 50 million euros for non-compliance.
[43] Germany: Media literacy and safe use of new media - European Commission

	Cyberbullying Law (Law 71/2017)	It targets cyberbullying among young people, mandating school prevention programmes, content removal, and support and rehabilitation services for both victims and perpetrators.
	'Red Code' Law ([44]) / 2019	It prioritises cases involving GBV, recognising the growing role of ICT in harassment cases by emphasising protections for victims in the digital sphere.
	Revenge Porn Law / 2019	Part of the 'Red Code' legislation, it criminalises the non-consensual sharing of intimate images or videos, with penalties of up to six years and increased sanctions for cases involving minors or intimate partners. It prioritises such cases, as well as other forms of GBV, to speed up proceedings and reduce victim trauma, while offering protections such as anonymous reporting, psychological support, and safeguards against retaliation.
Poland	Article 190a of the Penal Code / 2011	It criminalises stalking and harassment, including acts conducted via electronic means. Legal interpretations confirm that cyberstalking and cyberbullying are covered, even if the article does not explicitly use the term 'cyber'.
Portugal	Article 152 of the Penal Code / 2018	Law No. 44/2018 strengthened criminal protection of private life on the Internet. It introduced in paragraph 2(b) of Article 152 (domestic violence) the non-consensual dissemination via Internet or other widely accessible public media of personal data, including images or sound relating to private life as an aggravating form of domestic violence.
	Article 240 of the Penal Code / 2024	Law No. 4/2024, amended the Penal Code by adding a paragraph to Article 240, on discrimination and incitement to hatred. It specifies that if the offences are committed through a computer system, the court may order the deletion of the relevant data or content, extending legal protection against online or digital forms of hate speech and discrimination, including gender-based harassment.
	Penal Code	Under various general criminal provisions, Portuguese law criminalises invasion of privacy, crimes against the right to one's image, threats, stalking, and incitement to hatred or hate speech, and these provisions also apply when the offences occur online or through electronic means.
Romania	Criminal Code	Romania amended its Criminal Code to explicitly criminalise cyber harassment and cyberstalking, enhancing penalties in cases involving intimate partner violence. It also targets the non-consensual distribution of intimate content, imposing severe sanctions, particularly when the victim is a minor or the perpetrator is a close relation. Online hate speech is similarly penalised.

[44] Law no. 69/2019 aims at speeding up the judicial proceedings for specific types of crime, which are expression of domestic and gender-based violence.

	Amendments to Law 217/2003 on Preventing and Fighting Against Domestic Violence / 2020	Through the amendments, the law recognises cyber violence as a means of coercion and control, allowing protective measures such as prohibiting digital contact.

Embedding cyber violence protection in broader legal frameworks

A third trend is integrating cyber violence into broader legislation on gender-based violence, sexual offences, or child protection. In these cases, digital abuse is explicitly recognised as a form of coercion, discrimination, or violence, ensuring that online behaviours are treated as offline ones. These frameworks often include preventive and educational measures - particularly targeting schools and young people - alongside victim support services.

Table 3: Examples of provisions related to cyber violence added to existing national legal frameworks

Country	Name of the measure and year	Description
Belgium	Article 6 of the law of July 31, 2023 ([45])	The law amends article 584 ([46]) of the Judicial Code to streamline summary proceedings in cases of non-consensual distribution of sexually explicit content. Through an expedited procedure, victims can request a court order requiring the perpetrator(s) or the service provider to remove or render the images inaccessible. The law mandates that the president of the court of first instance ensures that the order contains all necessary data to identify the images or recording, facilitating their removal by service providers.
Cyprus	Law on the Prevention and Combating of Violence against Women and Domestic Violence / 2021	It criminalises the non-consensual publication or threat of publication of sexual or pornographic material through digital or other means.
	Protection from Harassment and Stalking Law (L.114(I)/2021)	It extends safeguards against harassment and stalking to online contexts.

([45]) Loi du 31/07/2023 visant a rendre la justice plus humaine, plus rapide et plus ferme iv

([46]) https://www.ejustice.just.fgov.be/cgi_loi/article.pl?language=fr&lg_txt=f&type=&sort=&numac_search=&cn_search=1967101003&caller=SUM&&view_numac=1967101003n

Sweden	Penal Code	Under Swedish Penal Code and related legislation, behaviours such as repeated online harassment, cyberstalking, and the non-consensual sharing of private or intimate content are criminalised. The principle that conduct deemed illegal offline is equally illegal online helps ensure consistency between digital and physical legal frameworks. For example, criminal liability for rape and sexual violence includes acts committed remotely, for example online.
	Reform to the Sexual Crimes Act / 2018	In 2018 the Swedish sexual offences legislation was reformed. It is now an offence to perform a sexual act with someone who is not participating voluntarily. Thus, to convict a perpetrator of rape it is no longer required to establish that violence or threats were used, or that the victim's particularly vulnerable situation was exploited.

5.2.2. Beyond legislative approaches at national level

While many EU MS have developed legislation targeting perpetrators of cyber violence, some have taken further steps by implementing policies and initiatives that offer victim support services and preventive measures. However, many of these approaches still lack a gender perspective that specifically considers the experiences of women and girls. As a result, these policies frequently fall short of offering a comprehensive response to gendered cyber violence against women and girls, who are disproportionately affected.

In some MS, policies to address cyber violence primarily focus on educational and awareness-raising measures and campaigns, often directed at the general public or at particularly affected groups such as women and young people. Some examples of initiatives are described in the table below.

Table 4: Examples of educational and awareness-raising measures in EU MS

Country	Title of the measure	Description
Austria	#GemeinsamGegenCybergewalt (Together Against Cyber Violence)	Launched in 2023-24, it focused on identifying victims' counselling needs and tailoring support services accordingly. The project produced counselling materials and informational resources for both victims and the public. Even after its official end, the network behind the initiative continues to share content on platforms like Facebook and Instagram, while providing updated guidance to counselling centres.
	Netzamazonen [47]	Led by the counselling service *Frauen beraten Frauen* (Women Advise Women), this project targets online dating safety, privacy, and smartphone security, and in 2024 published a handbook titled 'Is This Already Digital Violence?', offering a detailed analysis of the phenomenon.

[47] #netzamazonen website

Country	Title of the measure	Description
	Book for children on the internet risks	In cooperation with the Association of Internet Service Providers, Austria has produced an informational booklet in German, English, and Arabic to raise children's awareness of online risks.
Bulgaria	Cyberscout Programme [48]	Since 2015, this educational initiative aims at enhancing online safety awareness among children aged 11–12. Developed by the Bulgarian Safer Internet Centre (SIC), the programme aims to equip young students with the knowledge and skills to navigate the digital world safely.
Cyprus	Safer Internet Center – CYberSafety [49]	Developed by the Cyprus Pedagogical institute, it offers lectures and experiential workshops for students, teachers and parents to share information on safe and responsible use of internet and digital technologies. Since 2017, the Institute also organises summer camps focusing on internet safety and events around 'Safer Internet Day' every year in February.
Czechia	'Regions for a Safe Internet' campaign	Launched to raise awareness about online risks and promote preventive measures, targeting school children. Since 2019, Czech regions have collaborated on this initiative, which includes e-learning courses for children, students, teachers, parents, police officers, and social workers, as well as interactive online quizzes for students to test their knowledge of internet safety. The project also organises educational seminars.
	Training of police officers	Since 2023, over 400 police officers attended educational seminars on domestic and gender-based violence and gender-based cyberviolence designed for law enforcement.
Finland	'For you in social media' service [50]	Aimed at combating cyberbullying and online sexual abuse among young people aged 8 to 21. Operated by non-profit organisations, this service directly engages with youth on platforms where they often encounter cyber violence. Beyond individual support, the service actively produces educational content to raise awareness about online safety and healthy digital relationships. Their videos cover topics such as recognising and responding to cyberbullying, understanding consent, and navigating online interactions safely.
France	'StopCybersexisme' campaign	Launched in 2017, it aimed to raise awareness about digital sexual harassment and empower victims and witnesses with practical tools. It provides a toolkit comprising a poster, informational flyer, awareness video, and a dedicated website ([51]). This platform defines cybersexism, offers guidance for victims, promotes self-protection, and includes testimonials.

[48] Cyberscout Programme
[49] Trainings in schools - Internet Safety
[50] Sua Varten Somessa
[51] #Stopcybersexisme website

Country	Title of the measure	Description
	French Laboratory for Women's Rights Online	Established in 2024 as a platform for dialogue and innovation to tackle online violence against women, it also serves as incubator for concrete projects aimed at identifying, preventing, and curbing online and technology-facilitated gender-based violence.
	pHARe anti-harassment programme	Fully implemented since 2023 across all French schools, the programme tackles bullying through prevention, response mechanisms, and awareness. It includes the 3018 hotlines against online harassment in all student materials and trains staff to recognize and act on harassment. The central element of the programme is the "Non au harcèlement" school competition. This annual contest invites students to co-create anti-bullying campaigns, encouraging peer-to-peer involvement in promoting empathy, respect, and gender equality. The winner's campaign is promoted at national level in schools.
	"Parents, parlons numérique" awareness campaign	Launched by the Ministry for Solidarity, Autonomy and Equality, this campaign equips parents with tools and advice to help children develop healthy, respectful digital habits, especially in relation to online risks such as pornography and peer violence.
	Guide on intimate partner cyberviolence	The government has published a guide in 2025 for professionals in contact with women victims of gender-based violence, in partnership with the Centre Hubertine Auclert, a women's rights NGO that has expertise in cyberviolence.
	Association for the fight against sexist cyber violence (Echap)	Founded in 2020, it is a feminist association that addresses the rise of digital violence against women and marginalised groups. They work closely with domestic and sexual violence support organisations, providing technical assistance in cases involving spyware, online harassment, and privacy breaches. In addition, Echap develops accessible guides on digital threats and offers workshops.
Germany	Coordination Center for Digital Violence ([52])	This local initiative, launched by the organisation *Frauen helfen Frauen*, supports professionals who accompany victims of cyber violence - counsellors, women's shelter staff, and experts in the field of gender-based violence. The centre offers workshops that teach how digital abuse works and how it can be identified and stopped. Some seminars focus on practical issues like spyware and account security, while others deal with legal options and the challenges of privacy violations.
Hungary	NETMENTOR Peer Mentoring Programme [53]	Focused on promoting responsible internet use among young people through peer-to-peer mentoring, in order to understand its risks and possibilities. Among other activities, the NetMentor Programme trains older students to become 'NetMentors' who lead workshops for younger peers on topics like online privacy, digital footprints, and safe internet use. Educators are also trained to support and guide the mentors. The

[52] Koordinierungsstelle zu Digitaler Gewalt im sozialen Nahraum
[53] NETMENTOR programme

Country	Title of the measure	Description
		workshops are designed to be engaging and interactive, encouraging active participation and reflection on online behaviour.
Italy	'Stop Sexting and Revenge Porn' campaign	Campaign launched in 2021 by Mete Onlus to combat the non-consensual distribution of intimate images. It combined educational programmes, public awareness campaigns, and online resources to empower youth.
Latvia	Safety Messengers Programme	Launched by the State Police in 2022, it is a prevention initiative that engages educators and schools in teaching minors about safety risks and self-protection. Online violence and digital risks are specifically addressed through Interactive Role Plays designed for two age groups (8–10 and 11–14). These activities focus on different dangers in the online environment, including the risks of sexual abuse, how to recognise them, and recommendations for prevention.
	'Dangerous online friendship' tool	Developed in 2022 by the Safer Internet center in cooperation with State police and the Children Protection Center helpline, this online tool helps children, adolescents and educators recognise situations of grooming, receive advice and receive help ([54]).
Slovenia	Odklikni Project: Click-Off! Stop Cyber Violence Against Women and Girls	Implemented from 2017 to 2019, the project aimed to raise awareness among youth about digital GBV. The project included TV advertisements, posters, a mobile app, a dedicated website ([55]), and a manual for professionals working with young people. It also organised extensive training for educators, social workers, judges, and police officers, highlighting the need to avoid gender bias and stereotypes when addressing online violence. In parallel, other Slovenian projects focused on preventing dating violence among youth from a gendered perspective.
Spain	'PantallasAmigas' initiative ([56])	Established in 2004, it promotes the safe use of digital technologies among children and adolescents. It offers educational content on cyberbullying, grooming, sexting, and GBV online. Its Cyber managers programme uses peer-led approaches to foster digital responsibility.
	'#RedesSinMachismo' campaign ([57])	Media campaign launched in 2024 by the regional government of Andalusia to address the rise in digital gender violence.

Source: Author's elaboration

In addition to awareness-raising initiatives, there are some examples of some MS that have embedded actions targeting cyber violence into national action plans. These are seen in the table below.

Table 5: Examples of MS National action plans embedding cyber violence

Country	Title of the measure	Description

([54]) en.sos.drossinternets.lv
([55]) Odklikni project website
([56]) PantallasAmigas website
([57]) #RedesSinMachismo campaign

Austria	National Action Plan to Combat Violence against Women and Girls 2025-2029	It includes measures against digital violence, including AI. It contains a dedicated chapter on digital violence and addresses the implementation of the EU Directive on combating violence against women and domestic violence, including the criminal offences relating to cyber violence.
Belgium	National Action Plan to Combat Gender-Based Violence (2021–25)	It recognises the gendered nature of cyber violence and includes objectives to combat it through different measures such as an informational platform on cybersexism, improving police and judicial actions, and collaboration. The plan also supports law enforcement capacity-building and awareness campaigns targeting adult social media users.
Croatia	Action Plan for Violence Prevention in Schools (2020–24)	It includes measures targeting cyber sexual violence among children and youth. It supports school-based prevention programmes and defines specific forms of cyber violence, such as online hate speech, cyberstalking, cyber harassment, sexual harassment, and sexting.
Czechia	Gender Equality Strategy (2021–30) Action Plan for Prevention and Gender-Based Violence (2023-2026), Strategy for Criminality Prevention (2022-2027	Addresses cyber violence within partner violence. Highlights forms such as revenge porn and message harassment, especially affecting young people. Include measures such as training police on domestic and gender-based violence including cyberviolence and raising awareness on safe internet in schools.
Cyprus	-National Strategy for the Prevention and Combating of Violence Against Women (2023–28) -Cyprus National Cybersecurity Strategy 2020 -National Strategy for a Better Internet for Children in Cyprus (2018-2023)	The National Strategy calls for stricter media regulation and improved data collection, integrating GREVIO recommendations on online violence. The Cybersecurity Strategy includes measures to ensure the protection of critical information infrastructure, combat cyber threats and enhance resilience. The National strategy for a better internet for children in Cyprus includes actions concerning children, but also teachers, parents and the wider public.
France	-Fifth Plan to Mobilise and Combat Violence Against Women (2017-2019) -Interministerial Plan for Gender Equality (2023-2027)	It identifies young women as especially at risk of cyber violence. It includes a specific objective (Objective 24) to protect victims of cyber violence, particularly of cyber sexual harassment. Measures include compiling a list of police units trained in cybercrime and distributing a guide on legal protections and victim support options. Measures include improving the accessibility of complaint mechanisms and assistance for victims of cyberviolence and strengthening training tools

Italy	National Plan to Prevent Bullying and Cyberbullying at School (2016–17)	It established training programmes and awareness campaigns for students and teachers and introduced helplines for affected students and families. This has evolved over time, with updated provisions and the 'ELISA' platform offering e-learning for teachers handling cyberbullying cases.
Malta	Children's Policy Framework 2024-30	It includes targeted measures to address the heightened risks of cyber violence, recognising as well that girls are disproportionately affected. It tackles issues such as cyberbullying and online harassment.
Portugal	National Strategy for Equality and Non-Discrimination – Portugal + Equal (ENIND)	The national strategic plan to promote equality and combat discrimination provides three Action Plans. Under the Action Plan for the Prevention and Combating of Violence Against Women and Domestic Violence 2023-2026 (PAVMVD), it includes measures such as strengthening legal protection against forms of online violence, particularly image-based sexual violence targeting women and girls and online hate speech (Measure 242), and training and upskilling professionals to address these forms of online violence (Measure 418).

Source: Author's elaboration

Other MS have recognised the importance of cross-sector collaboration in addressing cyber violence. Some examples are seen in the table below.

Table 6: Examples of MS collaboration efforts in addressing cyber violence

Country	Title of the measure	Description
Czechia	'Be Safe' project	It addresses cyberbullying, also establishing a connection between schools, educational institutions, and the Police. Educators have access to up-to-date news and information on the latest trends in cyberbullying and cybercrime, which they can incorporate into their teaching.
Denmark	2017 Inter-ministerial Programme	Brought together the Ministries of Education, Justice, and Gender Equality to address digital sexual abuse. This initiative combined educational resources, public awareness campaigns, and partnerships with civil society organisations.
Estonia	*Targalt Internetis* (Smartly on the Web) programme ([58])	It integrates cybersecurity experts into educational efforts, providing young people with the tools and training needed to identify and respond to online threats, including GBV.
Germany	InterAktion project ([59])	Led by the Federal Association of Women's Shelters and Counselling Centres (bff), the project, launched in 2023, connects women's counselling centres and helplines with local IT professionals. By

[58] Smartly on the Web programme website
[59] InterAktion project

Country	Title of the measure	Description
		creating partnerships, these stakeholders address complex cases involving cyber violence.
Lithuania	Safer Internet Consortium	Collaborative model involving the IT Centre under the Ministry of Education and Science, the Communications Regulatory Authority, NGO Children's Line, and the digital literacy organisation Langas į ateitį. These partners have worked across sectors - including government, technology, media, and civil society - to create a safer digital environment for children and reduce their exposure to online risks.

Source: Author's elaboration

EU-level coordination and multistakeholder initiatives

At the EU level, collaborative efforts continue to drive progress. A key player in this effort is INHOPE, the International Association of Internet Hotlines, which began in 1999 with eight European hotlines and has since grown into a global network. It enables victims to report illegal online content, particularly child sexual abuse material, online grooming, and hate speech, including xenophobia. All EU MS are part of this network.

Another major initiative is INSAFE, which operates under the European Commission's BIK strategy. It runs Safer Internet Centres in 30 European countries, offering education and support through helplines and hotlines for children, parents, and teachers. These centres also forward reports of illegal or harmful online content to the appropriate authorities, such as internet service providers, law enforcement, or INHOPE hotlines. Importantly, they involve youth panels to ensure young people have a voice in shaping online safety policies and resources.

The EU also organises the annual Safer Internet Forum, bringing together policymakers, researchers, industry representatives, law enforcement, and young people to address online safety challenges. The 2024 forum focused specifically on cyber violence and protecting youth from harmful content and bullying. Similarly, Safer Internet Day, celebrated each year in over 100 countries, raises global awareness of issues like cyberbullying and online sexual harassment. The #SaferInternet4EU campaign, launched in 2018, furthers this mission by supporting EU-wide initiatives to address emerging digital risks.

Box 4: Examples of EU funded projects that promote a collaborative approach

CyberEqual project (2024): It is an Erasmus+ initiative involving Cyprus, Greece, Ukraine, Slovakia, and Lithuania. It aims at educating and raising awareness and prevention among young people about CVAWG). Its primary objectives include increasing knowledge on the prevalence and legislation of CVAWG, raising awareness and educating youth and professionals, motivating young to protect themselves, and equipping youth workers with tools to combat CVAWG.

Destalk (2021): it is a European initiative coordinated by Blanquerna-URL in Spain and Italy with support from the European Union's Rights, Equality and Citizenship programme. Its objective is to combat cyber violence and gendered cyber stalking. By 2022, the project had trained more than 350 professionals - primarily in Spain and

Italy - who work in the field of gender-based violence. DeStalk offers an online learning platform, creates practical tools and guidelines, and supports regional campaigns to raise awareness about cyber violence and digital safety.

Cybersafe project: Changing Attitudes among teenagers on Cyber Violence against Women and Girls (2019-2021)

The Cybersafe project was a 30-month European Union-funded initiative that brought together nine partners from various European countries – Italy, the Netherlands, United Kingdom, Denmark, Greece, Estonia, Slovenia, and Austria. Its primary goal was to develop, promote, and disseminate innovative educational tools to address cyber violence against women and girls among teenagers aged 13 to 16. Through the project a CYBERSAFE Toolkit was developed for teachers and other professionals working with young people, who want to address cyber violence against women and girls in the classroom or in other settings. The CYBERSAFE Toolkit offers resources and tools to organise and conduct four workshops addressing gender-based online violence. Its aim is to raise awareness and promote safe and responsible online behaviour among young people.

Targalt internetis project (2019)

The project aims to promote smarter internet usage among children and their parents while actively working to prevent the online distribution of child sexual abuse material. Co-financed by the European Commission, the initiative encompasses a variety of activities designed to enhance awareness and education. These include training sessions and seminars tailored for children, parents, teachers, and social workers, along with public awareness events aimed at the general population. Additionally, the project involves the creation of training materials that serve to inform children, teachers, and parents about safe internet practices. To engage children and students creatively, the project hosts competitions that encourage participation and awareness. Furthermore, it provides assistance and counselling through the Children's Helpline at 116111, accessible via telephone, MSN, and other instant messaging solutions, offering guidance to children and parents on the safe use of the internet and digital mobile devices. The initiative also features a web-based hotline which enables internet users to report environments containing materials that violate children's rights to sexual self-determination, as well as other inappropriate content. Since its inception in January 2019, the project has prioritised cooperation among various stakeholders in Estonia and across Europe, actively participating in the INHOPE and INSAFE networks to strengthen its impact.

DeSHAME (2017)

The DeSHAME project is an EU-funded project to prevent and respond to online sexual harassment. The project involved UK, Hungary, and Denmark, and aimed at addressing and reducing peer-based online sexual harassment among young people aged 13 to 17. The project sought to empower local communities to work together to increase reporting among young people. To deal with these issues, Project DeSHAME developed resources tailored for educators, parents, and young people. These materials aim to raise awareness, educate about the harms of online sexual harassment, and promote a safe online behaviour. The project also produced an International Adaptation Toolkit to assist other countries and organisations in implementing similar initiatives to tackle online sexual harassment.

Work With Perpetrators (2015)

The project provides valuable guidelines for addressing cyber violence, emphasising a perpetrator-focused approach. A key principle of these guidelines is that the burden of protection should not fall on the victim, as they have the fundamental right to safety in digital spaces. Instead of placing the responsibility on individuals to avoid or mitigate online abuse, the project underscores the need for systemic solutions, including stronger legal frameworks, proactive intervention strategies, and accountability measures for perpetrators. It also highlights the crucial role of collaboration among digital platforms, policymakers, and law enforcement in preventing and addressing cyber violence, ensuring that victims are not forced to endure harm in silence but are supported through comprehensive protections and effective enforcement mechanisms.

Other preventive measures in focus group countries

Analysing in-depth countries where focus groups were conducted, authorities and organisations have also implemented prevention-oriented strategies that aim to tackle cyber violence through targeted forms of support directed at children and young people, parents, and relevant institutions.

Parental guidance plays a crucial role in providing emotional support and practical advice to girls experiencing cyber violence. However, parents often face significant challenges in understanding how to best respond to such situations. In Germany and Italy, awareness-raising and prevention campaigns have been launched to promote safe internet use and to provide parents with guidance on how to support children and young people in dealing with issues related to cyber violence.

Box 5: Examples of campaigns for safer online environments: Germany and Italy

Germany's 'Klicksafe' campaign, co-funded by the EU, promotes responsible internet use among children, youth, parents, and educators. It includes specific resources to address digital sexual violence, such as the brochure 'The first smartphone – how can I protect my child from sexual violence on the internet?', produced in collaboration with the Federal Ministry for Family Affairs and the Independent Commissioner for Child Sexual Abuse Issues. Another major initiative is 'Active Against Digital Violence', which supports victims of gender-based digital abuse through awareness campaigns and practical tools, as part of Germany's broader digitalisation strategy.

In **Italy**, the initiative 'Scelgo io!' (I Choose), launched in 2018 by the organisation 'Cuore e Parole' and under the project 'Generazioni Connesse', offered online training and conferences for parents about the dangers of sexting among their children and provides guidance for protecting them from image-based abuse and cyber violence.

Source: author's elaboration through the 'Klicksafe' programme and 'Generazioni Connesse' websites

Other MS have adopted interesting practices to tackle cyber violence against young women and girls by integrating education, technology, and legal frameworks to foster a safer digital environment and prevent future incidents of cyber violence.

Box 6: Examples of practices for tackling cyber violence: Belgium, Ireland, Spain, and Estonia

Belgium's Plan Internationl initiative 'SafeHaven' uses Roblox (a popular online game platform) to sensitise young people about inappropriate behaviour in virtual worlds. Using interactive games set in an e-pavilion give them tools to break down stereotypes, set boundaries, and seek help. They are also encouraged to act as active bystanders both online and offline.

Ireland has integrated cyber-violence prevention into its school curriculum through the Social, Personal and Health Education (SPHE) short course. Updated in 2023, the programme includes modules on respectful online communication, digital consent, and recognising harmful behaviours in online interactions. It equips young people with practical knowledge and skills to prevent and respond to cyber harassment and image-based abuse.

Spain also took a creative approach with the 'Conectado' video game, which immerses players in the experience of a cyberbullying victim over five days to encourage empathy and dialogue in educational settings.

Estonia's web constables represent another innovative strategy, with police officers dedicated to monitoring and responding to online abuse, including hate speech and harassment.

Source: author's elaboration through 'SafeHaven'; Junior Cycle SPHE Curriculum, 'Conectado', and 'Web-constables' websites

Alongside parental guidance and integrated youth-centred and law enforcement measures, MS have implemented training programmes aimed at equipping teachers and specialised professionals with the skills to prevent and respond to online risks faced by children and young people. These initiatives recognise that schools and professional support services are often the first to detect signs of cyber violence.

Box 7: Examples of training programmes for teachers and specialised professionals: Cyprus, Poland, and Sweden

In **Cyprus**, specialised mental health staff such as educational psychologists are trained to assist children coping with online-related issues, particularly cyberbullying and digital anxiety, ensuring early and informed intervention.

In **Poland**, the Awareness Centre conducts webinars, classes, and workshops for teachers and other specialists focused on digital safety. In addition, the Empowering Children Foundation operates an online learning platform that provides open-access resources on internet safety for teachers.

Sweden's national 'Safe Internet Use' training module provides structured professional development for teachers, librarians, and school health personnel. Covering online behaviour, cyberbullying, gaming, and information security, it promotes collaborative learning and practical application in the classroom.

Source: author's elaboration through Polish Safer Internet Centre and Safe Internet Use-training module websites

5.2.3. Young people's perceptions of response

Although the insights presented here are based on **focus group discussions**—and are therefore **not intended to be generalised**—they constitute a **crucial and innovative contribution** to understanding how adolescents experience and respond to cyber violence. The discussion reveals a complex interplay between individual coping strategies, peer dynamics, institutional responses, and wider structural barriers. Participants' narratives highlight that experiences of shame, fear, and mistrust often prevent victims from reporting or seeking help. At the same time, schools, parents, and institutional actors are perceived as inconsistent or unprepared in their responses.

Individual responses

Girls' immediate emotional responses to cyber violence were shaped by age, perceived severity, and availability of support.

They often reacted with emotional withdrawal, silence, or blocking perpetrators, driven by fear, shame, or a desire to avoid escalation – such reactions were most common among younger girls (aged 13-15). Others described defensive confrontation, directly challenging aggressors online. Yet, even these active responses were often framed as last-resort reactions in the absence of supportive structures. Likewise, boys noted that shame - particularly in cases of image-based abuse - was a major barrier for girls in reporting incidents. Fear of judgment from parents or authority figures also emerged as a common key concern among girls and boys.

Nevertheless, for girls, parental guidance played a formative role in shaping how some of them approached online safety, especially during their early adolescence. Peers frequently played as well an important role as the first point of disclosure, offering emotional support, advice, and serving as a bridge to wider support networks.

Boys' accounts revealed a more mixed picture. Some described positive collaborations between parents and schools, while others feared blame and misunderstanding.

Institutional responses

Perceptions of institutional support - including schools and the police - were highly uneven. Parents were generally seen as more reliable and protective than other actors, though disclosure was often hindered by fear of disappointment or blame.

Older girls (aged 16 - 18) tended to express greater scepticism towards institutional responses. This scepticism often stemmed from personal negative experiences or heightened awareness of structural barriers, such as unhelpful counsellors. A widespread lack of awareness about existing support services for boys and girls also reinforced the belief that *'the solution lies within us, and not in seeking help'*.

Teachers and counsellors were seen as both potential allies and sources of frustration. Some boys valued trusted teachers who provided a safe space for disclosure. Others, however, expressed that some teachers exacerbated issues. Girls confirmed these feelings. For them, schools were frequently perceived as ineffective or dismissive. In many cases, trust in teachers was low, with several girls reporting that school staff downplayed or dismissed their experiences.

Some girls described feeling betrayed when counsellors promised confidentiality but later disclosed information to parents without consent. Others recounted positive experiences where teachers or counsellors intervened decisively, even if they were not always well-equipped or sufficiently trained to deal with cyber violence. This ambivalence underscores the variability in school responses, often dependent on individual staff rather than systemic approaches.

> 'The school counsellor never did anything. They just took notes and stuff. Then they called my parents and told them everything. And then I had to face my parents and take full responsibility. It was even worse. And that didn't just happen once. It happened more than once'. (Girl 16-18, Belgium)

Police were viewed by both girls and boys with greater scepticism and frustration, despite instances where authorities took action. Many participants doubted the seriousness with which authorities treated cyber violence, citing long delays, inaction, or outright dismissal. Boys, in particular, ridiculed the idea of involving the police.

'No one is going to call the police. Who's such a wimp that they'd call the police? Very few police officers would take this issue seriously'. (Boy 15-18, Cyprus)

Girls also reported frustration with ineffective investigations and delays.

'I was contacted two and a half years later... The complaint didn't really work out'. (Girl 16-18, Belgium)

Young people's views on adult support

Girls across countries and age groups generally view adults as disconnected from the realities of young people's digital lives. Many described adults - including parents and teachers - as lacking awareness, sensitivity, and training to respond effectively to cyber violence. Participants frequently reported that adults either downplay their experiences or respond in ways that discourage disclosure.

'Parents sometimes don't believe or like… generally older people don't believe us'. (Girl 13-15, Estonia)

'Many adults…around you tend to solve things by saying that it's not that important, when you feel that it is important and then it really hurts you'. (Girl 13-15, Romania)

Some girls expressed reluctance to seek help from parents, fearing punishment or misunderstanding rather than support. While some felt close to their parents and believed they could provide help, others emphasised that their parents lack understanding of the digital world. Other participants held adults accountable for early and excessive exposure to technology.

'I have acquaintances who received a phone with internet access at 3-4 years old… it seems to me that you got out of the womb and you were messed up by your parents, they just wanted you to shut up so they just gave you a tablet… now you don't know how to socialise, and you don't have communication skills and you're like, what am I doing here?'. (Girl 13-15, Romania)

The perceived role of teachers and school psychologists in prevention and intervention was mixed. Younger girls often trusted some teachers, particularly those who were kind or relatable. School psychologists were also mentioned as helpful. However, many participants

felt that schools lack genuine support mechanisms, with teachers and institutions often appearing indifferent or failing to act and, therefore, leading girls to think that *'school is the last place to ask for help'.*

The willingness of girls to seek adult support appears influenced by contextual factors. In some countries - such as Italy, Sweden, and Cyprus - they expressed greater disappointment in adult responses, whereas in others – such as Ireland and Estonia - girls were more inclined to trust adults, describing school and family as emotionally responsive or supportive.

Age also shapes perceptions of adult involvement. Younger girls (aged 13-15) were generally more open to confiding in trusted adults, particularly teachers and parents. Older participants (aged 16-18) were more sceptical, citing emotional distance, communication breakdowns, and generational differences, particularly regarding digital culture, sex, and relationships.

Limitations and young people's recommendations for effective prevention

Across countries, most girls agreed that prevention strategies are limited, outdated, or poorly implemented. School-based initiatives were often described as superficial, repetitive, and disconnected from young people's digital realities. Brief lectures, repeated campaigns, and school assemblies delivered by the same individuals were seen as largely ineffective.

Likewise, boys identified a critical gap in early and meaningful education on cyber violence, noting that current school-based interventions are often delivered too late or lack relevance.

Girls also reported that resources for preventing or responding to cyber violence are insufficient, particularly regarding support structures. Barriers to effective prevention included lack of confidentiality in small communities, vague or ineffective reporting mechanisms, insufficient age-appropriate education, and cultural taboos limiting open discussion. These challenges were especially pronounced among older girls (aged 16-18).

> 'Even if schools raise awareness of cyber violence, that is not effective because adults don't know how to reach teenagers'. (Girl 16-18, Italy)

Boys further called for stronger accountability for perpetrators, especially in addressing legal gaps related to image-based abuse, including deepfakes ([60]). This concern reflects an emerging theme within cyber violence, as online abuse in virtual reality (VR) and metaverse environments presents unprecedented challenges due to weak regulation, insufficient

([60]) In Ireland, creating a deepfake is not currently illegal, but distributing/resharing deepfakes is illegal under the Harassment, Harmful Communications and Related Offences Act 2020 (Coco's Law), explored in section 2.4.

moderation, and societal attitudes that minimise or dismiss online abuse as not 'real' (Chawki et al., 2024).

Girls proposed practical recommendations for improving prevention and support mechanisms, including:

- Improved access to mental health professionals;
- Anonymous and confidential reporting options;
- Peer-based online chat and support services;
- Support services that are visible, trustworthy, and emotionally accessible;
- More open and structured discussions in schools about cyber violence;
- Interactive, participatory, and experiential education using real-life examples;
- Clear and easily accessible information on how and where to report abuse;
- Prevention programmes that address both victims and perpetrators;
- Comprehensive training for teachers on how to communicate effectively with young people about sensitive topics.

6. Conclusions

CVAWG is a pervasive, deeply gendered continuum of violence - driven by unequal power relations and reinforced by social norms - that shapes and constrains the digital lives of girls and young women.

Cyber violence is a widespread, complex, and deeply gendered phenomenon that operates across both digital and physical environments, forming a continuum of abuse. It is rooted in societal norms, gender stereotypes and unequal power dynamics that reproduce offline hierarchies of gender and control within online spaces. These dynamics appear in behaviours that objectify, control, or silence girls and young women. They reflect wider social norms that reward male dominance and shame female sexuality. Among boys, certain acts of cyber violence are often condoned and seen as a way to gain approval from peers or prove masculinity, while girls who experience abuse are blamed or mocked. This creates a digital culture where aggression is linked to power, and responsibility for harm is shifted into victims.

Girls and young women experience cyber violence as a routine part of their digital and social lives, with distinct age-related patterns: younger girls (13–15) are more likely to face exclusion, gossip, and body shaming, while older girls (16–18) are more frequently subjected to sexualised forms of violence such as online sexual coercion and extortion, grooming, and non-consensual image sharing. Male teenagers are also found to be specifically targeted for online sexual coercion and extortion by perpetrators operating in organised criminal networks with financial gain being the main motivator.Younger adolescents are also increasingly exposed to sexualised and coercive forms of online abuse, underscoring the widening reach and normalisation of digital violence.

Evidence from focus groups further highlights that incidents of cyber violence often originate in offline settings such as schools, communities, or peer groups, and escalate online, spreading rapidly across multiple platforms and social arenas. This escalation between physical and digital spaces amplifies harm, blurs boundaries, and makes abuse harder to contain.

A diverse range of perpetrators, enablers, and passive bystanders sustains and amplifies the cycle of CVAWG.

Cyber violence is perpetrated by a wide range of actors, including peers, intimate partners, and organised groups. Digital anonymity enables and amplifies abuse, reducing accountability and enabling the spread of harmful behaviours. In addition to primary perpetrators, secondary actors who share and react to abusive content contribute significantly to its perpetuation. Bystanders also play a pivotal role: while some may intervene, many remain passive due to fear of reprisal and social pressure. The focus group findings show that boys, in particular, can act as both perpetrators and potential allies. Acts such as non-consensual image sharing or group harassment are often discussed as performances to impress others

or conform to peer expectations. This ambivalenceunderscores the need for greater efforts to cultivate empathy and accountability among bystanders.

Intersectional inequalities heighten vulnerability and deepen the impact of cyber violence among marginalised groups.

The findings underscore that cyber violence is shaped by intersecting identities and structural inequalities. Factors such as disability, ethnicity, religion, gender identity and socioeconomic status compound risk, with marginalised girls and young women facing higher exposure and fewer avenues for support. Focus groups' participants highlight how online spaces often reproduce offline systems of oppression – such as sexism, racism, and transphobic abuse - making certain groups more visible, targeted, and less protected. These inequalities not only increase the likelihood of experiencing cyber violence but also intensify its emotional and social consequences.

Systemic discrimination and unequal access to justice further exacerbate these vulnerabilities. Marginalised girls and young women often face significant barriers when seeking protection, including mistrust of institutions, lack of awareness about legal rights, and limited access to affordable legal assistance. Addressing CVAWG therefore requires an intersectional approach that recognises how overlapping forms of disadvantage amplify harm and perpetuate inequality.

Cyber violence has enduring psychological, emotional, and relational consequences that extend far beyond the digital realm, profoundly affecting victims' mental health, social trust, and sense of identity.

The continuum of cyber violence extends beyond the digital realm, leaving lasting psychological, emotional, and relational harm. The psychological and social impacts of such violence are profound, with victims frequently reporting high levels of anxiety, depression, trauma, and diminished self-esteem that have long-term consequences for mental health and relationships. Many adolescents describe experiences of social isolation and distrust, sometimes using terms such as 'depression', 'suicide', and 'trauma' to convey their distress. Fear of stigma, victim-blaming, and reputational damage further discourages reporting, thereby perpetuating cycles of silence.

The persistent presence of online abuse - with harmful content capable of resurfacing long after the initial event – means that its emotional, psychological, and relational effects remain deeply rooted and long-lasting. Moreover, beyond individual impacts, repeated exposure to online abuse also contributes to

the normalisation of violence. Young people begin to view cyberbullying and harassment as inevitable aspects of digital life, something to be endured rather than challenged. This normalisation not only magnifies the emotional toll of cyber violence but also entrenches patterns of acceptance and disengagement, reinforcing its enduring impact across both digital and social spheres.

The EU VAW/DV Directive provides a much-needed common framework in terms of definitions and enforcement mechanisms. Its full transposition and implementation should be prioritised to deliver results.

Efforts to address CVAWG are currently hampered by the high number of definitions used across countries and jurisdictions and by the rapid evolution of digital technologies, including AI. The diverse manifestations of cyber violence - ranging from harassment to image-based abuse – and the wide spectrum of motivations and relational dynamics that it entails require nuanced understanding and context-sensitive interventions. These must also account for broader cultural, institutional, and social factors including entrenched gender norms that normalise male aggression and victim-blaming, peer dynamics that reward abusive behaviour and reinforce double standards, the influence of online subcultures and pornography in shaping misogynistic attitudes, and institutional patterns that excuse boys' harmful conduct while failing to protect or believe girls.

The VAW/DV Directive provides clear definitions which can underpin the development of harmonised indicators, data collection processes, and monitoring and policy evaluation. As such it has potential to promote greater consistency and coordination across Member States.

Current prevention, education, and support systems do not reflect young people's digital realities, leading to isolation, lack of trust, and leaving many without effective protection.

Findings reveal a significant disconnect between existing prevention efforts and adolescents' lived experiences. During focus groups, girls expressed frustration with school-based campaigns, adult and parental responses, and institutional mechanisms that they perceived as outdated, superficial, or disconnected from their digital lives.

School campaigns about cyber safety are viewed as ineffective because they fail to engage with the actual platforms, practices, and risks young people encounter daily.

Adolescents consistently expressed that adults underestimate the significance of online spaces and the severity of the harm experienced there. Instead of acknowledging and validating these experiences, adults are often seen as minimising them. This lack of understanding deepens feelings of isolation and invalidation, particularly when young people seek help from institutions such as schools or counselling services. Many described inconsistent or poorly coordinated institutional responses, including breaches of

confidentiality and downplaying of their experiences, which erode trust and deter further disclosure.

This mismatch therefore undermines confidence in prevention and support mechanisms, discouraging reporting and leaving many adolescents without adequate protection. Structural barriers further compound the problem: young people often lack clear information about where to seek help, and in smaller communities, fear of exposure or gossip acts as a powerful deterrent.

Taken together, the findings highlight both progress and persistent challenges. CVAWG is firmly embedded within the continuum of gender-based violence and cannot be addressed in isolation from broader social, cultural, and institutional contexts. While EU policy has evolved to recognise the complexity and urgency of digital abuse, gaps in implementation and uneven responses across MS continue to limit effectiveness. Moving forward, coordinated, intersectional, and youth-centred approaches are essential to ensure meaningful prevention, protection, and accountability across the EU.

7. Policy recommendations

Combatting CVAWG across the EU requires coordinated, multi-level strategies and actions engaging both EU institutions and Member States. This requires alignment between EU directives, national legislation, and local implementation frameworks. The recommendations can be grouped into four interrelated areas.

Prevention and education

Guarantee early, gender-sensitive prevention that reflects girls' and boys' digital realities

- Introduce mandatory, gender-responsive digital literacy curricula in primary and secondary schools, covering digital identity, digital footprints, online interactions, and misinformation detection (including deepfakes and manipulated content). To this end, build on national examples whose positive impact has been demonstrated.
- Promote a culture of digital self-care in education institutions by raising awareness of students and educators on digital safety (privacy settings, safe documentation of evidence, reporting tools) by introducing regular "digital safety screenings" in schools, where students review their online presence and privacy settings with guided support.
- Include specific learning objectives for boys and young men on gender norms of masculinity, peer pressure, accountability and the role of complicity in cyber violence.
- Integrate evidence-based bystander intervention training into school curricula, youth work and digital literacy programmes, teaching young people how to safely intervene, report, disrupt, or support a peer being targeted online. To this end, build on successful bystander intervention programmes from specialised support services on violence against women.

Ensure prevention efforts are co-created with and responsive to girls' experiences

- Collaborate with youth-led and community-based civil society organisations, especially those working with diverse groups of youth, using participatory pedagogy build up on common intelligence, recognising young people's expertise in digital practices.
- Co-design prevention programmes with adolescents, ensuring that educational materials address cyber violence, including sexualised abuse, image-based violence, and victim-blaming narratives.
- Promote peer-led support initiatives where trained girls and boys can discuss harassment, coercion, and healthy digital relationships, creating safe spaces to share experiences.

- Ensure girls' and boys' participation in co-creation does not translate into responsibility-shifting towards victims. To this end, thrive to provide a safe space for their voices and expertise while ensuring that victim receive professional specialised support.
- Provide parents and caregivers with practical guidance on digital parenting, including tools and resources to help families detect and address online abuse early.

Challenge harmful gender norms and address intersecting risks

- Develop targeted programmes for boys that challenge sexist social norms and offer positive alternatives through role models, mentorship, and youth-led discussions on respect, consent, and healthy relationships. Such programmes can build on and be integrated in comprehensive sexuality education (CSE) curricula.
- Target outreach to girls facing intersecting discrimination (e.g. migrant girls, girls with disabilities, LGBTIQ+ youth) to address their specific online risks and barriers to support.

Integrate prevention into broader EU and national policy frameworks

- Fund structured youth advisory panels to inform national and EU-level prevention strategies.
- Fund EU-wide campaigns featuring girls' voices to destigmatise reporting of intimate image abuse and highlight the harms of perpetrating and sharing such content.
- Ensure that prevention of online gender-based violence is fully implemented and enforced through existing EU legislation and policy frameworks, including the European Commission's Action Plan Against Cyberbullying ([61]), the Digital Services Act (DSA), EU Strategy on the Rights of the Child, the EU Youth Strategy, and the Violence Against Women Directive [62].

Encourage and support technological innovations to improve prevention

- Promote responsibility into platform and product design to anticipate ways platforms technical features can be misused for abuse.
- Ensure that social media platforms invest in the development of innovative technological solutions to anticipate, detect and deter acts of cyberviolence specifically targeting girls and young women.

([61]) Action plan against cyberbullying – protecting children online | Shaping Europe's digital future

- Ensure that platforms strengthen deterrence through both messaging (e.g., pop-up warnings before sharing non-consensual images) and technical tools (e.g., image-based detection systems that flag potential violations). Such measures can shape user behaviour proactively and have a strong preventive function.
- Mandate proactive detection and moderation of harmful trends, especially those targeting girls and LGBTQIA+ youth.

Develop EU wide cooperation on Image Hashing and Non-Consensual Image Databases

- Building on existing initiatives such as StopNCII.org, facilitate collaboration between ENISA, national cybersecurity centres, and trusted third-party organisations.
- Support the interoperability and standardisation of image hashing databases to enable consistent detection and removal of harmful content across platforms.
- Ensure that victim reporting mechanisms at national levels are directly linked to these technical infrastructures, so that once an image is hashed and flagged, it is recognised and blocked across multiple services.

Legal and policy framework on cyber violence

Ensure robust, harmonised regulation and enforcement across the EU

- Reaffirm the EU's political will and commitment to enforce and build on existing legal frameworks especially the Digital Services Act (DSA), the AI Act and the GDPR. In the context of the ongoing discussions on the Digital Omnibus Package, uphold core safeguards.
- Ensure full enforcement of the Digital Services Act (DSA), and the full transposition and implementation of the AI Act and the Directive on combating violence against women and domestic violence (EU VAW/DV Directive), including gender-specific obligations for prevention, reporting and victim support.
- Employ common, harmonised definitions of the different forms of cyber violence set by the EU VAW/DV directive and the CVAWG measurement framework developed by EIGE to facilitate the collection of comparable, sex-disaggregated EU-wide data on online gender-based violence.
- Commend and pursue the full coordination between national institutions and the European Board for Digital Services to monitor and improve social media platforms' compliance with the DSA requirements.
- Disseminate and encourage adherence to the European Commission's guidelines on protecting minors online adopted in July 2025.

Strengthen Member States cybersecurity awareness and protocols to better respond to cyber violence

- Develop EU wide clear referral routes for support services at national level to access technical expertise — whether through national cybersecurity centres, CSIRTs, or law enforcement units. Such expertise would equip practitioners to respond to tech-facilitated abuse cases with appropriate technical support.
- Build on expertise at EU level for example ENISA to strengthen these links by promoting consistent technical guidance, training, and cross-border information sharing.
- Develop mutual learning and information sharing at EU level on national initiatives.
- Develop an EU protocol for responding to cyberviolence in schools, detailing steps for documentation, reporting, evidence preservation, and cross-stakeholder collaboration.

Mandate strong platform accountability and victim-friendly reporting tools

- Promote strong mechanisms to monitor social media platforms' compliance with the DSA and the EU directive on combating violence against women and domestic violence especially in terms of moderation practices, reporting and support to users. The establishment of an independent monitoring body could provide useful coordination and oversight.
- Increase the number and visibility of EU-approved trusted flaggers / trusted third parties to facilitate rapid reporting and escalation of illegal content.
- Involve specialised support services on violence against women in the development of user-centred, anonymous and accessible mechanisms to report incidents of cyber violence to digital platforms– including hotlines, mobile apps and online portals.
- Ensure that reporting mechanisms address the intersectional dimension of cyber violence. In particular, the needs and reporting behaviour of users of different age groups, especially younger ones should be taken into account to maximise accessibility of reporting.
- Ensure that DSA takedown obligations are implemented with clear timeframes and proactive notification to victims once content is removed.
- Incentivise platforms to adopt and adhere to a Code of Conduct on combating gender-based cyber violence, developed in cooperation with civil society and equality bodies.

Set stronger standards for safer platform design and proactive risk mitigation

- Promote the creation of stronger platform standards that account for the real-life harms women and girls face online, including requirements for:
    - Safe product and algorithmic design, to reduce the amplification of harmful content and prevent re-victimisation.

- Sound risk assessment and safeguarding strategies, ensuring platforms actively identify and address risks such as online harassment, deepfakes, and image-based abuse.

- Require trauma-informed and victim-centred design principles in moderation processes and interface design.
- Introduce mandatory gender impact assessments as part of fundamental rights assessments under the AI Act, including third-party audits to detect and correct algorithmic bias.
- Align platform age-verification, design and user-safety requirements with the European Commission's 2025 Guidelines and prototype app for a safer online space for children.
- Ensure that these age-verification measures are implemented in a gender-sensitive way, recognising that girls face distinct risks in online settings.

Strengthen and ensure the enforcement of regulation of AI and emerging technologies

- Ensure the enforcement of the AI act.
- Ensure that existing EU AI governance instruments — including the Ethics Guidelines for Trustworthy AI and Codes of Practice on Generative AI — are fully implemented and strengthened with binding accountability mechanisms.
- Advocate for gender-related risks of generative AI such as the production and dissemination of deepnudes, nudifying tools and other non-consensual synthetic imagery to be listed as 'prohibited practices' under Article 5 of the AI Act.
- Ensure that technical standards developed for AI providers include effective mechanisms for reporting complaints and following up, removing harmful content and informing victims of cyber violence about support services.
- Ensure that equality bodies and civil society organisations working towards gender equality and fundamental rights at national and EU level are sufficiently equipped and financed to fulfil their role of consultative bodies under Article 77 of the AI act.
- Ensure remedies and mechanisms are accessible to victims of AI-enabled violence.

Victim's support and protection

Strengthen victim-centred support services and reporting mechanisms

- Ensure that all Member States implement reporting and support services for victims of cyber violence – in line with existing obligations under the Istanbul Convention (Art. 20–22), the Victims' Rights Directive (2012/29/EU) and the EU Directive on combating violence against women and domestic violence linked to rapid response and specialised support services.

- Ensure that specialised support services on violence against women are sufficiently equipped and financed to provide specialised, trauma-informed support, including technical support, mental health services and legal assistance.
- Ensure that specialised support for victims of cyber violence is tailored to different age groups of women and girls, based on their experiences and needs.
- Develop age-appropriate perpetrator intervention programmes specifically tailored for minors, recognising their developmental stage and differing accountability mechanisms.

Strengthen professional capacity to respond effectively

- Provide mandatory training to frontline professionals (teachers, social workers, police, healthcare workers) on the gendered nature of cyberviolence and platform-specific patterns.
- Establish national technical assistance points, allowing practitioners to access cybersecurity expertise from public institutions or specialised civil society organisations.
- Ensure sustainable funding to civil society organisations conducting school interventions and for those specialising in digital and gender equality awareness work for young people to prevent cyberviolence and generative AI deepfakes.

Support families, caregivers and educators in early intervention and response

- Provide parents and caregivers with practical guidance on digital parenting, including tools and resources to help families detect and address online abuse early.
- Require schools and other educational institutions to establish clear policies and protocols on what to do in cases of technology-facilitated abuse, to protect victims.
- Require schools and other educational institutions to define and communicate clear consequences for perpetrators of cyber violence (e.g., disciplinary records, or notes on school reports, temporary or permanent expulsion and what is proposed in this case).
- Raise awareness of parents and care givers of civil legal avenues for victims to seek accountability and civil remedies.

Foster multi-stakeholder collaboration and innovation

- Facilitate cooperation between governments, civil society, researchers, schools and other education centres, and technology companies by promoting the sharing of evidence and best practices across stakeholders to improve prevention and response.

- Introduce EU-level multi-stakeholder response protocols for schools and youth settings, clarifying roles of educators, police, social services, platforms, and cybersecurity bodies.
- Support the development of innovative technological solutions tailored to the rapidly evolving nature of cyber violence.

Monitoring and evaluation

Establish a harmonised EU monitoring and accountability framework

- Ensure that National Action Plans are used to systematically track Member State implementation of the Directive on combating violence against women and domestic violence, including its provisions on prevention, protection, access to justice and cyber violence.
- Ensure regular evaluation of Member State compliance to guarantee harmonised standards, identify enforcement gaps, and support corrective action where obligations under the Directive are not met.
- Advocate for the European Commission to issue periodic monitoring reports on cyber violence, based on Member State data collection obligations under the VAW Directive and the DSA.

Ensure data collection reflects the diversity of victims' experiences

- In collaboration with relevant institutions at EU- and national level, collect disaggregated data on all forms of gender-based violence, including cyber violence, by sex, age, ethnicity, disability, and socioeconomic status.
- Ensure that the specific experiences of groups facing intersecting forms of discrimination are captured in research and data collection.
- Ensure that cyber violence and other forms of technology-facilitated forms of violence against women are integrated in future EU-wide victimisation surveys.

Invest in long-term, evidence-based research on impacts and trends

- In line with Article 44 of the VAW/DV Directive, ensure adequate budget allocation for specific research on cyber violence under current and future Multiannual Financial Framework (MFF).
- Support longitudinal research to understand the long-term psychological impacts of cyber violence.
- Investigate the social and economic consequences of cyber violence over time.

References

Adam, A. (2002) 'Cyberstalking and Internet pornography: Gender and the gaze', *Ethics and Information Technology*, 4(2), pp. 133–142. Available at: https://doi.org/10.1023/A:1019967504762.

Afrouz, R. and Vassos, S. (2024) 'Adolescents' Experiences of Cyber-Dating Abuse and the Pattern of Abuse Through Technology, A Scoping Review', *Trauma, Violence, & Abuse*, 25(4), pp. 2814–2828. Available at: https://doi.org/10.1177/15248380241227457.

Allen, C. and McIntosh, V. (2023) *Child safeguarding and immersive technologies: an outline of the risks.* London: NSPCC.

Allison, K.R., Bussey, K. (2016) Cyber-bystanding in context: A review of the literature on witnesses' responses to cyberbullying. Children and Youth Services Review. 65. 10.1016/j.childyouth.2016.03.026.

Almenar, R. (2021) 'Cyber Violence against Women and Girls: Gender-based Violence in the Digital Age and Future Challenges as a Consequence of Covid-19', *European Journal of Developmental Psychology*, 9(2), pp. 260–274. Available at: https://doi.org/10.1080/17405629.2011.643170.

Amnesty International (no date) *What is online violence?*, *Amnesty International*. Available at: https://www.amnesty.org/en/what-we-do/technology/online-violence/.

Assemblée nationale (2019) *Lutte contre la haine sur internet*, *Assemblée nationale*. Available at: https://www.assemblee-nationale.fr/dyn/15/dossiers/lutte_contre_haine_internet.

Azzarito, L., Simon, M., & Marttinen, R. (2017) 'Up against Whiteness': Rethinking race and the body in a global era. Sport, Education and Society, 22(5), 635–657. https://doi.org/10.1080/13573322.2015.1136612

Baas, de Jong and Drossaert (2013) *Children's Perspectives on Cyberbullying: Insights Based on Participatory Research.*

Backe, E.L., Lilleston, P. and McCleary-Sills, J. (2018) 'Networked Individuals, Gendered Violence: A Literature Review of Cyberviolence', *Violence and Gender*, 5(3), pp. 135–146. Available at: https://doi.org/10.1089/vio.2017.0056.

Barlińska, J., Szuster, A., & Winiewski, M. (2013). "Cyberbullying among adolescent bystanders: Role of the communication medium, form of violence, and empathy." *Journal of Community & Applied Social Psychology*, **23**(1), 37–51. → Empirical article; DOI: 10.1002/casp.2137

Baroncelli, L. (2020) 'Same Violence, New Tools: How to work with violent men on cyber violence', publication has been produced with the financial support of the "Rights, Equality and Citizenship Programme 2014-2020" of the European Union https://www.work-with-perpetrators.eu/fileadmin/wwp/Learn/Guidelines__manuals___policies/How_To_Cyber_Violence.pdf

Bitensky, S.H. (2010) 'Council of Europe Convention on the Protection of Children Against Sexual Exploitation and Sexual Abuse', *International Legal Materials*, 49(6), pp. 1663–1682. Available at: https://doi.org/10.5305/intelegamate.49.6.1663.

Brudvig, I., Chair, C., & van der Wilk, A. (2020) 'Covid-19 and increasing domestic violence against women: The pandemic of online gender-based violence'.

Calderón Gómez, D. and Puente, H. (2024) *Generación expuesta Jóvenes frente a la violencia sexual digital.*

CfDP (2020) *The angry internet. A threat to gender equality, democracy & well-being*, Centre for Digital Youth Care https://cfdp.dk/wp-content/uploads/2020/11/CFDP_the_angry_internet_ISSUE.pdf

Chawki, M., Basu, S., & Choi, K.-S. (2024). Redefining Boundaries in the Metaverse: Navigating the Challenges of Virtual Harm and User Safety. https://www.mdpi.com/2075-471X/13/3/33

Chiang, J., Chang, F. and Lee, K. (2021) 'Transitions in aggression among children: Effects of gender and exposure to online violence', *Aggressive Behavior*, 47(3), pp. 310–319. Available at: https://doi.org/10.1002/ab.21944.

Connell, R. W. (2005). *Masculinities* (2nd ed.). Cambridge: Polity Press. → Foundational sociological text on hegemonic masculinity.

Cosma, A., Molcho, M. and Pickett, W. (2024) 'A focus on adolescent peer violence and bullying in Europe, central Asia and Canada', Volume 2. Copenhagen: WHO Regional Office for Europe; Available at: https://www.who.int/europe/publications/i/item/9789289060929

Council of Europe (2001) *Convention on Cybercrime*. Available at: https://rm.coe.int/1680081561.

Council of Europe (2007) 'Council of Europe Convention on the Protection of Children Against Sexual Exploitation and Sexual Abuse'. Available at: https://www.coe.int/en/web/conventions/full-list?module=treaty-detail&treatynum=201.

Council of Europe (2011) *Council of Europe Convention on preventing and combating violence against women and domestic violence*. Available at: https://rm.coe.int/168008482e.

Council of Europe (2018) *Mapping study on cyberviolence*. Available at: https://rm.coe.int/t-cy-2017-10-cbg-study-provisional/16808c4914

Council of Europe (2019a) *First Edition of Member state responses to prevent and combat online child sexual exploitation and abuse.*

Council of Europe (2019b) *Mechanisms for collective action to prevent and combat online child sexual exploitation and abuse.*

Council of Europe (2020) *Handbook for policy makers on the rights of the child in the digital environment.*

Council of Europe (2021) *Second Edition of Member state responses to prevent and combat online child sexual exploitation and abuse.*

Council of Europe (2022) *Second Additional Protocol to the Convention on Cybercrime on enhanced co operation and disclosure of electronic evidence*. Available at: https://www.coe.int/en/web/cybercrime/second-additional-protocol/-/asset_publisher/isHU0Xq21Ihu/content/opening-coecyber2ap.

Council of Europe (2023) *Risks and opportunities of the metaverse*.

Council of Europe (no date) *GREVIO Baseline Evaluation Reports on Action against Violence against Women and Domestic Violence*.

Craig, W. *et al.* (2020) 'Social Media Use and Cyber-Bullying: A Cross-National Analysis of Young People in 42 Countries', *The Journal of Adolescent Health: Official Publication of the Society for Adolescent Medicine*, 66(6S), pp. S100–S108. Available at: https://doi.org/10.1016/j.jadohealth.2020.03.006.

CYBERSAFE project (2019) Initial Consultations with Teenagers on Cyber Violence against Women and Girls: Analysis of Local Target Group Perspectives.

Cybersafe project (2020) *Cyber Violence against Women & Girls REPORT*.

De Keseredy, W. S., & Schwartz, M. D. (2013). *Male Peer Support and Violence Against Women: The History and Verification of a Theory.* Boston: Northeastern University Press. → The "male peer support" theory text, discussing how peer dynamics discourage intervention.

De Vido, S. (2024) *Deep fake as AI-generated violence against women*.

DeKeseredy, W.S. (2021) 'Image-Based Sexual Abuse: Social and Legal Implications', *Current Addiction Reports*, 8(2), pp. 330–335. Available at: https://doi.org/10.1007/s40429-021-00363-x.

Deutsche Gesellschaft für Internationale Zusammenarbeit (2022) *The influence of gender-based online violence on political and societal participation of women and girls*.

Domínguez-Hernández, F., Bonell, L. and Martínez-González, A. (2018) 'A systematic literature review of factors that moderate bystanders' actions in cyberbullying', *Cyberpsychology: Journal of Psychosocial Research on Cyberspace*, 12(4). Available at: https://doi.org/10.5817/CP2018-4-1.

Dunn, S. (2020) *Technology-Facilitated Gender-Based Violence: An Overview.* Centre for International Governance Innovation. Available at: https://www.jstor.org/stable/resrep27513.

EIGE (2018) 'Gender equality and youth: opportunities and risks of digitalisation'.

EIGE (2022a) *Artificial intelligence, platform work and gender equality.* Available at: https://eige.europa.eu/publications-resources/publications/artificial-intelligence-platform-work-and-gender-equality-report?language_content_entity=en.

EIGE (2022b) *Combating Cyber Violence against Women and Girls*. Available at: https://eige.europa.eu/sites/default/files/documents/combating_cyber_violence_against_women_and_girls.pdf.

EIGE (2024) *Tackling cyber violence against women and girls: The role of digital platforms*.

EIGE (2025) *Perception to policy: Dismantling gender stereotypes in the European Union*. Available at: https://eige.europa.eu/publications-resources/publications/perception-policy-dismantling-gender-stereotypes-european-union?language_content_entity=en

Estrada Tanck, D. (2024) 'Cyberspace and women's human rights in the international legal order: Transnational risks and gender-based violence', *Cuadernos de derecho transnacional*, 16(1), pp. 192–207. Available at: https://doi.org/10.20318/cdt.2024.8420.

European Commission (2016) *Code of conduct on countering illegal hate speech online*. Available at: https://commission.europa.eu/strategy-and-policy/policies/justice-and-fundamental-rights/combatting-discrimination/racism-and-xenophobia/eu-code-conduct-countering-illegal-hate-speech-online_en.

European Commission (2020) *Communication from the Commission to the European Parliament, the Council, the European Economic and Social Committee and the Committee of the Regions A Union of Equality: Gender Equality Strategy 2020-2025*. Available at: https://ec.europa.eu/newsroom/just/items/682425/en.

European Commission (2021) *European equality law review: European network of legal experts in gender equality and non-discrimination*.

European Commission (2024) *Digital Decade Policy Programme 2030*.

European Commission (2025) *The Code of conduct on countering illegal hate speech online + | Shaping Europe's digital future*. Available at: https://digital-strategy.ec.europa.eu/en/library/code-conduct-countering-illegal-hate-speech-online.

European Court of Auditors (2019) 'Challenges to effective EU cybersecurity policy'. Available at: https://www.eca.europa.eu/lists/ecadocuments/brp_cybersecurity/brp_cybersecurity_en.pdf.

European Parliament (2012) *Directive 2012/29/EU of the European Parliament and of the Council of 25 October 2012 establishing minimum standards on the rights, support and protection of victims of crime, and replacing Council Framework Decision 2001/220/JHA* Available at: https://eur-lex.europa.eu/eli/dir/2012/29/oj/eng.

European Parliament (2016) *General data protection regulation (GDPR) | EUR-Lex*. Available at: https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=legissum:310401_2.

European Parliament (2018) 'Directive (EU) 2018/ 1808 of the European Parliament and of the council - of 14 November 2018 - amending Directive 2010/ 13/ EU on the coordination of certain provisions laid down by law, regulation or administrative action in Member States concerning the provision of audiovisual media services (Audiovisual Media Services Directive) in view of changing market realities'. Available at: https://eur-lex.europa.eu/legal-content/EN/TXT/PDF/?uri=CELEX:32018L1808.

European Parliament (2021a) *European Parliament resolution of 14 December 2021 with recommendations to the Commission on combating gender-based violence: cyberviolence*

(2020/2035(INL)). Available at: https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=oj:JOC_2022_251_R_0002.

European Parliament (2021b) *Regulation (EU) 2021/1232 of the European Parliament and of the Council of 14 July 2021 on a temporary derogation from certain provisions of Directive 2002/58/EC as regards the use of technologies by providers of number-independent interpersonal communications services for the processing of personal and other data for the purpose of combating online child sexual abuse*. Available at: https://eur-lex.europa.eu/eli/reg/2021/1232/oj/eng.

European Parliament (2022a) *Proposal for a Regulation of the European Parliament and of the Council laying down rules to prevent and combat child sexual abuse*. Available at: https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=CELEX:52022PC0209.

European Parliament (2022b) *Regulation (EU) 2022/2065 of the European Parliament and of the Council of 19 October 2022 on a Single Market For Digital Services and amending Directive 2000/31/EC (Digital Services Act)*. Available at: https://eur-lex.europa.eu/eli/reg/2022/2065/oj/eng.

European Parliament (2024a) Artificial Intelligence Act. Available at: https://eur-lex.europa.eu/eli/reg/2024/1689/oj/eng.

European Parliament (2024b) 'Cyberbullying among young people: Laws and policies in selected Member States'.

European Parliament (2024c) 'Cyberviolence against women in the EU'. Available at: https://www.europarl.europa.eu/RegData/etudes/BRIE/2024/767146/EPRS_BRI%282024%29767146_EN.pdf.

European Parliament (2024d) *Directive (EU) 2024/1385 of the European Parliament and of the Council of 14 May 2024 on combating violence against women and domestic violence*. Available at: https://eur-lex.europa.eu/eli/dir/2024/1385/oj/eng.

European Parliament. Directorate General for Parliamentary Research Services. (2024) *Combating child sexual abuse: Revising Directive (2011/93/EU)* Epithintank, 24 July 2024. Available at: https://epthinktank.eu/2024/07/24/combating-child-sexual-abuse-revising-directive-2011-93-eu-recast-eu-legislation-in-progress/

European Parliament. Directorate General for Parliamentary Research Services. (2021) *Combating gender-based violence: cyber violence : European added value assessment.* LU: Publications Office. Available at: https://data.europa.eu/doi/10.2861/23053.

European Union Agency for Fundamental Rights (ed.) (2015) *Violence against women: an EU-wide survey main results*. Vienna, Austria: FRA, European Union Agency for Fundamental Rights.

European Union Agency for Fundamental Rights (ed.) (2017) *Second European Union minorities and discrimination survey: Muslims: selected findings*. Luxembourg: Publications Office. Available at: https://doi.org/10.2811/072254.

European Union Agency for Law Enforcement Cooperation (2017) *Online sexual coercion and extortion as a form of crime affecting children / Law enforcement perspective*. Available at: online_sexual_coercion_and_extortion_as_a_form_of_crime_affecting_children.pdf

European Women's Lobby (EWL) (2017) *#HerNetHerRights: Mapping the state of online violence against women & girls in Europe*.

European Women's Lobby (EWL) (2024) *Report on Cyber Violence Against Women*.

FEMM Committee (2018) 'Cyber violence and hate speech online against women'.

Freed, D., Consolvo, S., Cosley, D., Kelley, P. G., Ricart, E., Thomas, K., & Bazarova, N. N. (2025) *Help-seeking and Coping Strategies for Technology-facilitated Abuse Experienced by Youth*.

French Government (2022) *LOI n° 2022-299 du 2 mars 2022 visant à combattre le harcèlement scolaire (1)* (2022) *2022-299*. Available at: https://www.legifrance.gouv.fr/jorf/id/JORFTEXT000045287658#:~:text=%2DAucun%20%C3%A9l%C3%A8ve%20ou%20%C3%A9tudiant%20ne,ou%20mentale%20ou%20de%20d%C3%A9grader.

French Government (2023) *LOI n. 2023-566 du 7 juillet 2023 visant à instaurer une majorité numérique et à lutter contre la haine en ligne* (2023). Available at: https://www.legifrance.gouv.fr/download/pdf?id=uixn4vDFFJU_veW4xSVamq3PzXyh2U2x_naRfEud_Wg=.

Gámez-Guadix, M., Sorrel, M. A., & Martínez-Bacaico, J. (2022) Technology-Facilitated Sexual Violence Perpetration and Victimization Among Adolescents: A Network Analysis.

Gius, C. (2023) '(Re)thinking gender in cyber-violence. Insights from awareness-raising campaigns on online violence against women and girls in Italy', *Media Education*, 14(2), pp. 95–106. Available at: https://doi.org/10.36253/me-14896.

Government of Belgium (2021) *Plan d'action national de lutte contre les violences basées sur le genre 2021-2025. Axes stratégiques et mesures clés*. Available at: https://sarahschlitz.be/wp-content/uploads/sites/300/2021/11/20211125-PAN-2021-2025-clean-FR.pdf.

Government of Croatia (2020) *Akcijski plan za prevenciju nasilja u Školama*. Available at: https://mzom.gov.hr/UserDocsImages/dokumenti/StrucnaTijela/Akcijski%20plan%20za%20prevenciju%20nasilja%20u%20skolama%20za%20razdoblje%20od%202020.%20do%202024.%20godine.pdf.

Government of Denmark (2017) *Stepping up initiatives against digital sexual abuse*. Available at: https://rm.coe.int/2-meeting-draft-group-rec-sexism-info-doc-stepping-up-initiatives-agai/168072b9e8.

Government of the Czech Republic (2021) *Gender Equality Strategy for 2021 ur 2030: Updated version*. Available at: https://vlada.gov.cz/assets/ppov/rovne-prilezitosti-zen-a-muzu/dokumenty/Updated-Gender-Equality-Strategy-2021-2030---Condensed-Version.pdf

GREVIO (2021) *GREVIO General Recommendation No. 1 on the digital dimension of violence against women adopted on 20 October 2021*. Available at: https://rm.coe.int/grevio-rec-no-on-digital-violence-against-women/1680a49147.

Gurumurthy, A. (2009) 'Violence against Women via Cyberspace', *Economic and Political Weekly* [Preprint].

Hicks, J. (2021) *Global Evidence on the Prevalence and Impact of Online Gender-based Violence (OGBV)*. Institute of Development Studies (IDS). Available at: https://doi.org/10.19088/K4D.2021.140.

Hinduja, S. and Patchin, J.W. (2024) *Metaverse risks and harms among US youth: Experiences, gender differences, and prevention and response measures*.

International Center for Research on Women (ICRW) (2018) *Technology-Facilitated Gender-Based Violence: What Is It, And How Do We Measure It?*

Janickyj, M., & Tanczer, L. M. (2025). Tech Abuse Personas: Exploring Help-Seeking Behaviours and Support Needs of Victim/Survivors of Technology-Facilitated Abuse. *Proceedings of the Extended Abstracts of the CHI Conference on Human Factors in Computing Systems*, 1–11. https://doi.org/10.1145/3706599.3719986

Koukopoulos, N., Janickyj, M., & Tanczer, L. M. (2025) Defining and Conceptualizing Technology-Facilitated Abuse ("Tech Abuse"): Findings of a Global Delphi Study.

Leonhardt, M., Overå, S. (2021) Are There Differences in Video Gaming and Use of Social Media among Boys and Girls?—A Mixed Methods Approach.

Liao, Y. (2023) 'The Research on Primary Factors and Consequences of Adolescent Cyberbullying on Social Media Platforms', *Lecture Notes in Education Psychology and Public Media*, 3(1), pp. 362–369. Available at: https://doi.org/10.54254/2753-7048/3/2022503.

López-Castro, L. and Priegue, D. (2019) 'Influence of Family Variables on Cyberbullying Perpetration and Victimization: A Systematic Literature Review', *Social Sciences*, 8(3), p. 98. Available at: https://doi.org/10.3390/socsci8030098.

López-Castro, L. *et al.* (2023) 'Age differences in bullying victimisation and perpetration: Evidence from cross-cultural surveys', *Aggression and Violent Behavior*, 73, p. 101888. Available at: https://doi.org/10.1016/j.avb.2023.101888.

Lu, Y., Van Ouytsel, J. and Temple, J.R. (2021) 'In-Person and Cyber Dating Abuse: A Longitudinal Investigation', *Journal of social and personal relationships*, 38(12), pp. 3713–3731. Available at: https://doi.org/10.1177/02654075211065202.

Lumsden, K. and May Morgan, H. (2017) *Cyber-trolling as symbolic violence: deconstructing gendered abuse online*.

Machado, B. *et al.* (2022) 'Mapping the Cyber Interpersonal Violence among Young Populations: A Scoping Review', *Social Sciences*, 11(5), p. 207. Available at: https://doi.org/10.3390/socsci11050207.

Martínez-Soto, A., Ibabe, I (2024). Cyber Dating Abuse: Conceptualization and Meta-analysis of Prevalence Rates.

McGraw, D.K. (1995) *Sexual Harassment in Cyberspace: The Problem of Unwelcome E-mail*. Available at: https://heinonline.org/HOL/LandingPage?handle=hein.journals/rutcomt21&div=18&id=&page=.

Mclocklin, G., Kellezi, B., Stevenson, C., & Mackay, J. (2024) Disclosure Decisions and Help-Seeking Experiences Amongst Victim-Survivors of Non-Consensual Intimate Image Distribution. Victims & Offenders, 0(0), 1–27. https://doi.org/10.1080/15564886.2024.2329107

Min Bae, S. (2024) *Characteristics and Treatment of Cyberviolence Trauma in Children and Adolescents*.

Ministère des familles, de l'enfance et des droites des femmes (2017) *Le sexisme tue aussi. 5eme plan de mobilisation et de lutte contre toutes les violences faites aux femmes 2017-2019*. Available at: https://www.cipdr.gouv.fr/wp-content/uploads/2018/01/5%C3%A8me-plan-de-mobilisation-et-de-lutte-contre-toutes-les-violences-faites-aux-femmes-2017-2019-1.pdf.

MIUR (2016) *Piano Nazionale per la prevenzione del bullismo e del cyber-bullismo a scuola 2016/2017*. Available at: https://www.istruzione.it/allegati/2016/Piano_azioni_definitivo.pdf.

Moretti, C. and Herkovits, D. (2021) 'De víctimas, perpetradores y espectadores: una meta-etnografía de los roles en el ciberbullying', *Cadernos de Saúde Pública*, 37(4), p. e00097120. Available at: https://doi.org/10.1590/0102-311x00097120.

Mukred, M. *et al.* (2024) 'The roots of digital aggression: Exploring cyber-violence through a systematic literature review', *International Journal of Information Management Data Insights*, 4(2), p. 100281. Available at: https://doi.org/10.1016/j.jjimei.2024.100281.

Nadhiroh, A.M. *et al.* (2023) 'Multi-Dimensional Impact of Cyber Gender-Based Violence: Examining Physical, Mental, Social, Cultural, and Economic Consequences', *Gaceta Médica de Caracas*, 131(4S). Available at: http://saber.ucv.ve/ojs/index.php/rev_gmc/article/view/27115.

National Academies of Sciences, Engineering, and Medicine. (2024) The Relation between Social Media and Health, in: Social Media and Adolescent Health. National Academies Press (US).

Nixon, C.L. (2014) 'Current perspectives: the impact of cyberbullying on adolescent health', *Adolescent Health, Medicine and Therapeutics*, 5, pp. 143–158. Available at: https://doi.org/10.2147/AHMT.S36456.

O'Brien, M. (2024) *Online violence: real life impacts on women and girls in humanitarian settings*, *Humanitarian Law & Policy Blog*. Available at: https://blogs.icrc.org/law-and-policy/2024/01/04/online-violence-real-life-impacts-women-girls-humanitarian-settings/.

OAS (2021) 'Online gender-based violence against women and girls: Guide of basic concepts'.

OECD (2021) *Children in the digital environment: Revised typology of risks*.

Olenik-Shemesh, D., Heiman, T. and Eden, S. (2017) 'Bystanders' Behavior in Cyberbullying Episodes: Active and Passive Patterns in the Context of Personal-Socio-Emotional Factors', *Journal of Interpersonal Violence*, 32(1), pp. 23–48. Available at: https://doi.org/10.1177/0886260515585531.

Penado-Abilleira, M. and Rodicio-García, M.L. (2018) 'Development and Validation of an Adolescent Gender-Based Violence Scale (ESVIGA)', *Anuario de Psicología Jurídica*, 28(1), pp. 49–57. Available at: https://doi.org/10.5093/apj2018a10.

Pichel, R., Foody, M., O'Higgins Norman, J., Feijóo, S., Varela, J., Rial, A. (2021) Bullying, Cyberbullying and the Overlap: What Does Age Have to Do with It?

Pietkiewicz, M. and Treder, M. (2018) 'Cyberstalking in social media – Polish view', *Journal of Modern Science*, 38, pp. 29–40. Available at: https://doi.org/10.13166/jms/99217.

PLAN International (2020) *State of the World's Girls 2020: Free to Be Online?*

Powell, A., & Henry, N. (2017). *Sexual Violence in a Digital Age*. London: Palgrave Macmillan. → Academic monograph analysing digital contexts of sexual and gendered violence. DOI: 10.1057/978-1-137-57744-2

Pozza, V.D. *et al.* (2024) '*Report on Cyber Violence against women. Policy overview and recommendations, European Women's Lobby*

Project deSHAME (2017) *Young people's experiences of online sexual harassment: a cross-country report.*

Ratajczak, M. and Galzignato, E. (2019) *Migrant Children and Cyber-violence. The Problem of Hate Speech in Italy and Poland.*

Ray, A. (2024). *Sextortion: A Scoping Review.*

Rigotti, C. and Malgieri, G. (2024) *Sexual violence and harassment in the metaverse: A new manifestation of gender-based harms.* Alliance for Universal Digital Rights, Equality Now and The International Observatory on Vulnerable People in Data Protection (Vulnera).

Rodríguez Ramos, M.S. and Zarzalejos, J. (2024) 'Revision of the victims' rights acquis'. Available at: https://www.europarl.europa.eu/legislative-train/theme-a-new-push-for-european-democracy/file-revision-of-the-victims-rights-acquis.

Rudnicki, K. *et al.* (2023) 'Systematic review of determinants and consequences of bystander interventions in online hate and cyberbullying among adults', *Behaviour & Information Technology*, 42(5), pp. 527–544. Available at: https://doi.org/10.1080/0144929X.2022.2027013.

Safer Internet Centre Lithuania (2019) *Safer Internet Centre in Lithuania: Annual report 2019-2020.* Available at: https://www.draugiskasinternetas.lt/wp-content/uploads/2021/03/English_2019-2020.pdf.

Sala, A., Porcaro, L., Gómez, E. (2024) Social Media Use and adolescents' mental health and well-being: An umbrella review.

Salazar, M. *et al.* (2023) 'Cyber Sexual Harassment among Adolescent Girls: A Qualitative Analysis', *Adolescents*, 3(1), pp. 84–91. Available at: https://doi.org/10.3390/adolescents3010007.

Sales, N.J. (2024) 'A girl was allegedly raped in the metaverse. Is this the beginning of a dark new future?', *The Guardian*, 5 January. Available at: https://www.theguardian.com/commentisfree/2024/jan/05/metaverse-sexual-assault-vr-game-online-safety-meta.

Sánchez-Jiménez, V., Rodríguez-deArriba, M.-L. and Muñoz-Fernández, N. (2022) 'Is This WhatsApp Conversation Aggressive? Adolescents' Perception of Cyber Dating Aggression', *Journal of Interpersonal Violence*, 37(19–20), pp. NP17369–NP17393. Available at: https://doi.org/10.1177/08862605211028011.

Schittenhelm, C., Kops, M., Moosburner, M., Fischer, M.S., Wachs, S. (2024) Cybergrooming Victimization Among Young People: A Systematic Review of Prevalence Rates, Risk Factors, and Outcomes.

Sciacca, B. *et al.* (2023) 'Nonconsensual Dissemination of Sexual Images Among Adolescents: Associations With Depression and Self-Esteem', *Journal of Interpersonal Violence*, 38(15–16), pp. 9438–9464. Available at: https://doi.org/10.1177/08862605231165777.

Scott, A., Semmens, L. and Willoughby, L. (2001) 'Women and the Internet: The natural history of a research project', in *Virtual Gender*. Routledge.

Secretariat of the Lanzarote Committee (2018) *Guidelines for Implementation of Child Participation.* Available at: https://rm.coe.int/guidelines-for-implementation-of-child-participation/1680790571.

Singh, P., Smith, M.V., Raba, C.M., Keller, J. (2016) Cyber-Intimate Partner Violence and Mental Health Outcomes in a Sample of High School Girls. MOJPH 4. https://doi.org/10.15406/mojph.2016.04.00078

Smahel, D. *et al.* (2020) *EU Kids Online 2020: Survey results from 19 countries,* Doi: 10.21953/lse.47fdeqj01ofo.

Smith, A. (2024) *Rape in virtual reality: How to police the metaverse | Context*. Available at: https://www.context.news/digital-rights/sex-assault-claims-and-crime-raise-fears-of-new-virtual-wild-west.

Smith, D.-N. (2023) How Deception Plays a Role in Online Dating and Dating Apps.

Sourander, A. *et al.* (2010) 'Psychosocial risk factors associated with cyberbullying among adolescents: a population-based study', *Archives of General Psychiatry*, 67(7), pp. 720–728. Available at: https://doi.org/10.1001/archgenpsychiatry.2010.79.

Steinvik, H.R., Duffy, A.L. and Zimmer-Gembeck, M.J. (2023) 'Bystanders' Responses to Witnessing Cyberbullying: the Role of Empathic Distress, Empathic Anger, and Compassion', *International Journal of Bullying Prevention* [Preprint]. Available at: https://doi.org/10.1007/s42380-023-00164-y.

Šulc, A. *et al.* (2024) '(PDF) Differences in Cyberbullying Victimisation and Perpetration According to Age and Locality in Slovenia', *ResearchGate* [Preprint]. Available at: https://www.researchgate.net/publication/364723601_Differences_in_Cyberbullying_Victimisation_and_Perpetration_According_to_Age_and_Locality_in_Slovenia.

Sutton, S., & Finkelhor, D. (2023) Perpetrators' Identity in Online Crimes Against Children: A Meta-Analysis. Trauma, Violence, & Abuse, 25(3), 1756–1768. https://doi.org/10.1177/15248380231194072

The Economist Intelligence Unit (2021) *Measuring the prevalence of online violence against women, Jigsaw Infographic*. Available at: https://onlineviolencewomen.eiu.com/.

The Law Library of Congress (2019) *Laws Protecting Journalists from Online Harassment*. Available at: https://maint.loc.gov/law/help/protecting-journalists/online-harassment.pdf.

Torek, B. (2025, January 15). Meta's New Policies: How They Endanger LGBTQ+ Communities and Our Tips for Staying Safe Online. HRC. https://www.hrc.org/news/metas-new-policies-how-they-endanger-lgbtq-communities-and-our-tips-for-staying-safe-online

UN Women (2021) *A Guide for Women and Girls to Prevent and Respond to Cyberviolence*.

UN Women (2022) 'Accelerating efforts to tackle online and technology facilitated violence against women and girls (VAWG)'.

UN Women and World Health Organization (2023) *Technology-facilitated violence against women: Taking stock of evidence and data collection*. Available at: https://www.unwomen.org/en/digital-library/publications/2023/04/technology-facilitated-violence-against-women-taking-stock-of-evidence-and-data-collection.

UN Women (2024a) *Technology-facilitated gender-based violence: Developing a shared research agenda*. Available at: https://www.unwomen.org/en/digital-library/publications/2024/09/technology-facilitated-gender-based-violence-developing-a-shared-research-agenda.

UN Women (2024b) *Toolkit: Youth guide to end online gender-based violence*.

UNESCO (2021) *The Chilling: Global trends in online violence against women journalists*.

UNESCO (2023) *'Your opinion doesn't matter, anyway': exposing technology-facilitated gender-based violence in an era of generative AI*.

United Nations (2018) *A/HRC/38/47: Report of the Special Rapporteur on violence against women, its causes and consequences on online violence against women and girls from a human rights perspective, OHCHR*. Available at: https://www.ohchr.org/en/documents/thematic-reports/ahrc3847-report-special-rapporteur-violence-against-women-its-causes-and.

United Nations (2024) *Cyberviolence Against Women and Girls: The Growing Threat of the Digital Age, United Nations Western Europe*. Available at: https://unric.org/en/cyberviolence-against-women-and-girls-the-growing-threat-of-the-digital-age/.

United States Agency for International Development (2023) *DRG Learning Digest - Combatting Technology-Facilitated Gender-Based Violence in Politics, United States Agency for International Development*. Available at: https://content.govdelivery.com/accounts/USAIDHQ/bulletins/34c7e57.

Vallance, C. (2024) 'Police investigate virtual sex assault on girl's avatar', 2 January. Available at: https://www.bbc.com/news/technology-67865327.

Van Ouytsel, J., Ponnet, K. and Walrave, M. (2020) 'Cyber Dating Abuse: Investigating Digital Monitoring Behaviors Among Adolescents From a Social Learning Perspective', *Journal of Interpersonal Violence*, 35(23–24), pp. 5157–5178. Available at: https://doi.org/10.1177/0886260517719538.

Vogels, E.A. (2022) 'Teens and Cyberbullying 2022', *Pew Research Center*, 15 December. Available at: https://www.pewresearch.org/internet/2022/12/15/teens-and-cyberbullying-2022/.

Vogler, S., Kappel, R., & Mumford, E. (2023) Experiences of Technology-Facilitated Abuse Among Sexual and Gender Minorities. Journal of Interpersonal Violence, 38(19–20), 11290–11313. https://doi.org/10.1177/08862605231179724

Waasdorp, T.E. and Bradshaw, C.P. (2014) *The Overlap Between Cyberbullying and Traditional Bullying*.

Wajcman, Judy (2004). *TechnoFeminism*. Polity Press.

Wajcman, Judy (2010). "Feminist Theories of Technology." *Cambridge Journal of Economics*, 34(1), 143–152.

Wajcman, Judy (2015). *Pressed for Time: The Acceleration of Life in Digital Capitalism*. University of Chicago Press.

Wallace, A., Langevin, R. and Hébert, M. (2023) 'An Analysis of Risk and Protective Factors Associated with Cyber-Dating Violence Victimization of Adolescent Girls: An Ecological Perspective', *Journal of Child & Adolescent Trauma*, 16(4), pp. 1017–1029. Available at: https://doi.org/10.1007/s40653-023-00558-6.

WeProtect Global Alliance (2020) *Preventing and tackling child sexual exploitation and abuse: A Model National Response.*

WeProtect Global Alliance (2021) *Child 'self-generated' sexual material online: Children and young people's perspectives.*

World Wide Web Foundation (2024) *Perpetrators of gender-based violence online: roadmap for investigations.*

World Wide Web Foundation and World Association of Girl Guides and Girls Scouts (2020) *Survey - Young people's experience of online harassment*. Available at: https://ureport.in/opinion/3983/.

Wright, M.F. (2017) 'Adolescents' Perceptions of Popularity-Motivated Behaviors, Characteristics, and Relationships in Cyberspace and Cyber Aggression: The Role of Gender', *Cyberpsychology,*

Behavior and Social Networking, 20(6), pp. 355–361. Available at: https://doi.org/10.1089/cyber.2016.0693.

Wright, M.F. (2020) 'The Role of Technologies, Behaviors, Gender, and Gender Stereotype Traits in Adolescents' Cyber Aggression', *Journal of Interpersonal Violence*, 35(7–8), pp. 1719–1738. Available at: https://doi.org/10.1177/0886260517696858.

Wright, M.F. and Wachs, S. (2020) 'Adolescents' Cyber Victimization: The Influence of Technologies, Gender, and Gender Stereotype Traits', *International Journal of Environmental Research and Public Health*, 17(4), p. 1293. Available at: https://doi.org/10.3390/ijerph17041293.

Xu, Y. and Trzaskawka, P. (2021) 'Towards Descriptive Adequacy of Cyberbullying: Interdisciplinary Studies on Features, Cases and Legislative Concerns of Cyberbullying', *International Journal for the Semiotics of Law*, 34(4), pp. 929–943. Available at: https://doi.org/10.1007/s11196-021-09856-4.

Yoon, J. (2022). Can We Do Anything About Sexual Crimes in the Metaverse? https://blogs.luc.edu/compliance/?p=4849

Zweig, J.M. *et al.* (2014) 'Correlates of cyber dating abuse among teens', *Journal of Youth and Adolescence*, 43(8), pp. 1306–1321. Available at: https://doi.org/10.1007/s10964-013-0047-x.

Annex

Boxes

Box 8: Detailed methodological approach carried out for the study

DESK RESEARCH AND LITERATURE REVIEW

The initial stage of the study consisted of systematic desk research and literature review, which provided the conceptual and empirical grounding for the study. Key studies and policy documents were identified using databases such as Google Scholar and Semantic Scholar. While Google Scholar was used for broad initial screening, Semantic Scholar enabled a more targeted search through AI-supported recommendations and citation analysis. Relevance to the study's objectives and publication date (with priority given to 2019–2024) were key inclusion criteria. Earlier works were included when necessary to trace the evolution of debates or to provide historical depth.

The review encompassed a wide range of sources: peer-reviewed articles, academic books, reports produced by international and European institutions (e.g. EIGE, UN, World Bank), studies from NGOs and EU-wide women's rights organisations (e.g. European Women's Lobby, WAVE), as well as project outputs from EU-funded research. Grey literature, including documents from associations, specialised journals, and press articles, was also incorporated to capture ongoing debates and emerging concerns. Zotero software was used to manage references and classify literature according to keywords and themes. Tags allowed us to group studies by specific research questions or methodological approaches, ensuring a well-structured and retrievable evidence base.

MAPPING OF POLICY MEASURES AND LEGAL PROVISIONS

Building on the literature review, the study carried out a systematic mapping of relevant policy frameworks and legal provisions at international, European, and national levels. This mapping aimed to identify the regulatory architecture addressing cyber violence and to highlight convergences and divergences among Member States. The process drew on a wide range of official sources, including the European Court of Human Rights (HUDOC) database, GREVIO monitoring reports, the Council of Europe online library, EIGE's legal definitions repository, and the European Forum of Official Gazettes.

Snowball techniques further ensured that national laws and emerging policy measures were captured beyond the initial sample of documents. This approach provided a comprehensive picture of the policy and legal landscape in the EU, emphasising both common trends and specific national approaches.

STATISTICAL DATA ANALYSIS

Quantitative analysis helped contextualise the research by examining the prevalence and dynamics of cyber violence across Member States. At the EU level, this drew on statistics from Eurostat's survey on gender-based violence (EU-GBV), the FRA/EIGE survey on violence against women, and the Health Behaviour in School-aged Children (HBSC) study.

National surveys and data collected by NGOs and umbrella organisations, were also examined. International comparative surveys (e.g. Plan International, Pew Research Center) added further perspective, while EU-funded projects such as EU Kids Online provided detailed insights into children's and adolescents' online behaviours. The triangulation of these sources allowed the study to quantify trends and situate the qualitative findings within wider structural dynamics.

FOCUS GROUPS AND QUALITATIVE DESIGN

The second pillar of the methodology was qualitative fieldwork, designed to capture the lived experiences of adolescents in their own voices. A total of 37 focus groups were conducted across ten EU Member States (Belgium, Cyprus, Estonia, Germany, Ireland, Italy, Poland, Romania, Spain, and Sweden), involving 133 girls aged 13–18 and 38 boys aged 15–18. The decision to use focus groups was grounded in feminist and participatory principles: participants were not treated merely as informants, but as knowledge-holders capable of articulating the ways in which gendered power relations and social norms shape their experiences of online harm.

Group discussions were structured around tailored discussion guides, adapted to different age groups. For younger participants (13–15), the discussion guides included interactive activities (e.g. word clouds, games such as Kahoot) and a vignette about a fictional character experiencing cyber harassment, to encourage reflection without requiring personal disclosure. For older adolescents (16–18), the discussion guides included more complex scenarios, such as pressure to share intimate images and subsequent online harassment, allowing for deeper engagement with themes of digital consent and reputational harm. The focus groups with boys focused on social norms, masculinity, bystander behaviour, and empathy. In line with the project's ethics and safeguarding policy, discussions with boys and girls also addressed potential support mechanisms available after experiences of cyber violence. Recruitment strategies ensured diversity in socio-economic background, ethnicity, and educational settings, while prioritising psychological safety. Focus groups were held in youth-

friendly and accessible venues such as schools, community centres, and libraries. Informed parental consent and participant assent were obtained in all cases.

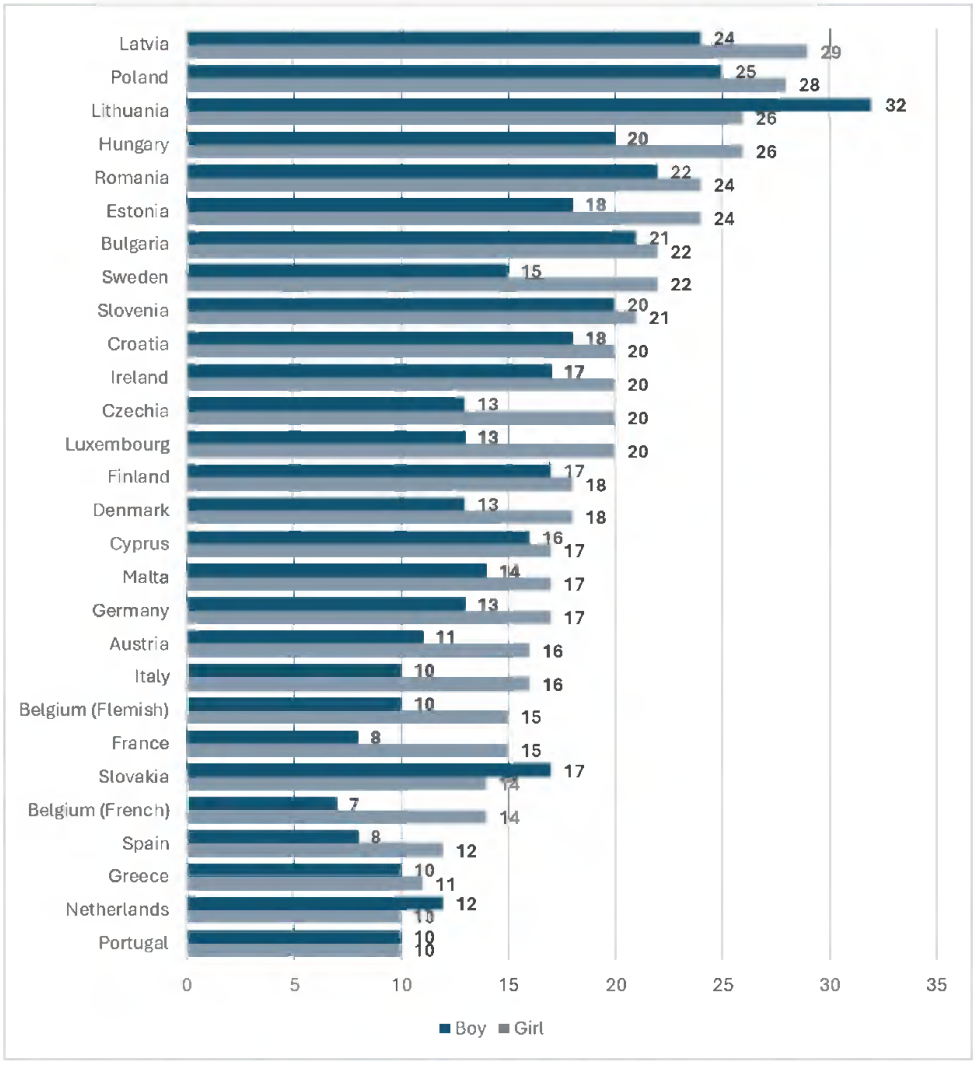
Data analysis was carried out through a combined thematic and synthesis approach. Focus group discussions were transcribed, coded, and analysed using NVivo software. Coding categories included forms of cyber violence, perceived causes, impacts, coping strategies, barriers to reporting, and institutional responses. Coding was both inductive, allowing new themes to emerge directly from the data, and deductive, guided by predefined research questions and the study's theoretical framework.

Thematic analysis was complemented by synthesis analysis to compare findings across age groups and countries, enabling the identification of shared patterns as well as contextual variations. Triangulation with quantitative data and policy findings further reinforced the robustness of the analysis. This multi-layered framework ensured that adolescents' subjective accounts were interpreted against the backdrop of structural evidence.

Given the sensitive nature of the research and the participation of minors, strong ethical safeguards were applied. The study was conducted in compliance with WHO guidelines and institutional child protection frameworks. Informed consent and assent procedures were central to the design: guardians received detailed information on the study's objectives and procedures, while adolescents were given the agency to assent or withdraw at any point. Safeguarding measures included trained facilitators, confidentiality guarantees, and continuous monitoring of participants' wellbeing before, during, and after the sessions.

Figures

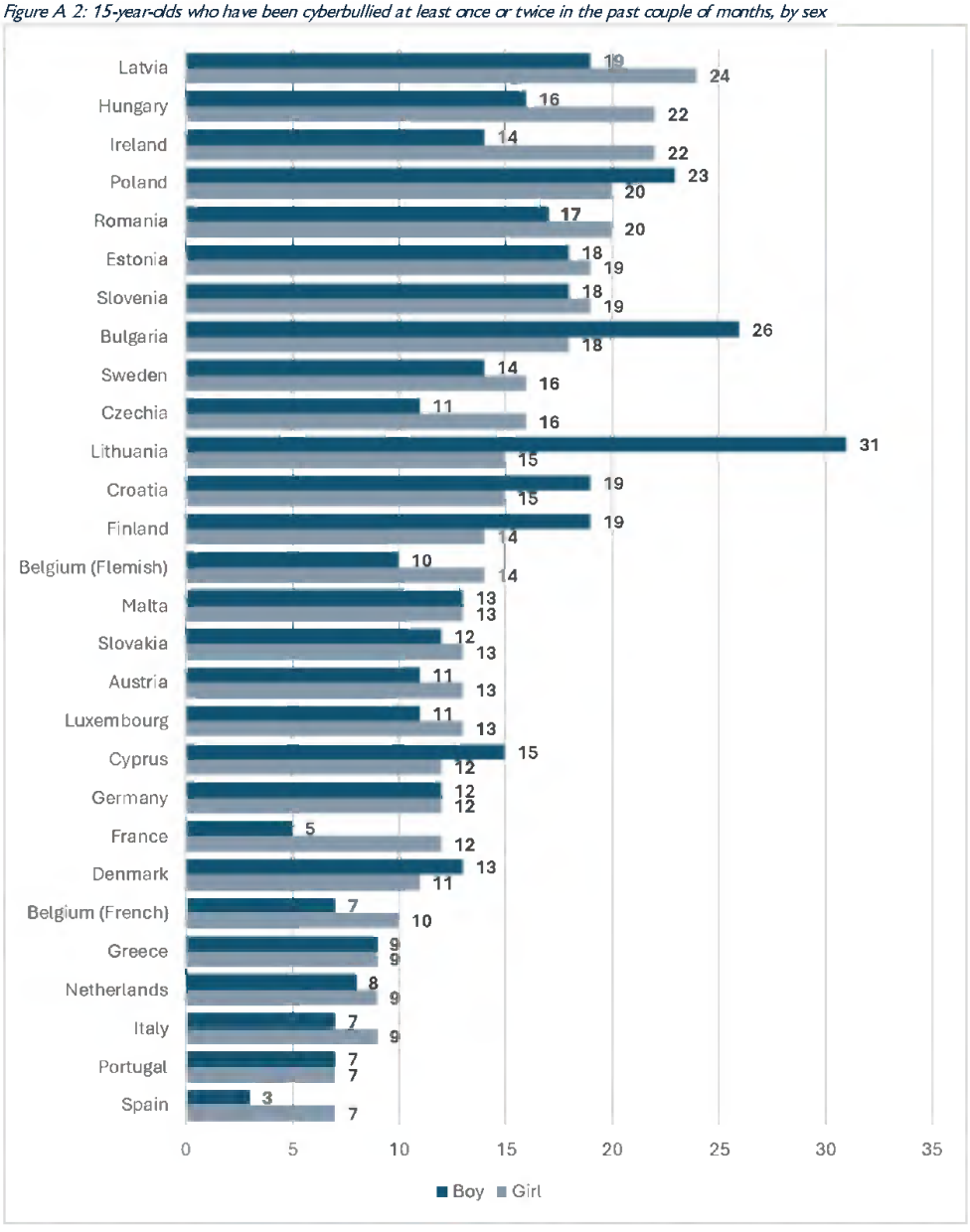
Figure A 1: 13-year-olds who have been cyberbullied at least once or twice in the past couple of months, by sex



Note: *Young people were asked how often they had experienced cyberbullying (e.g. anyone sending mean instant messages wall postings or emails or someone posting or sharing photos or videos online without their permission). Response options ranged from I have not been cyberbullied in the past couple of months to several times a week. Findings presented here show the proportions who had experienced cyberbullying at least once or twice a month in the past couple of months.*

Source: Health Behaviour in School-aged Children study (2023), Data browser (findings from the 2021/22 international HBSC survey): https://data-browser.hbsc.org

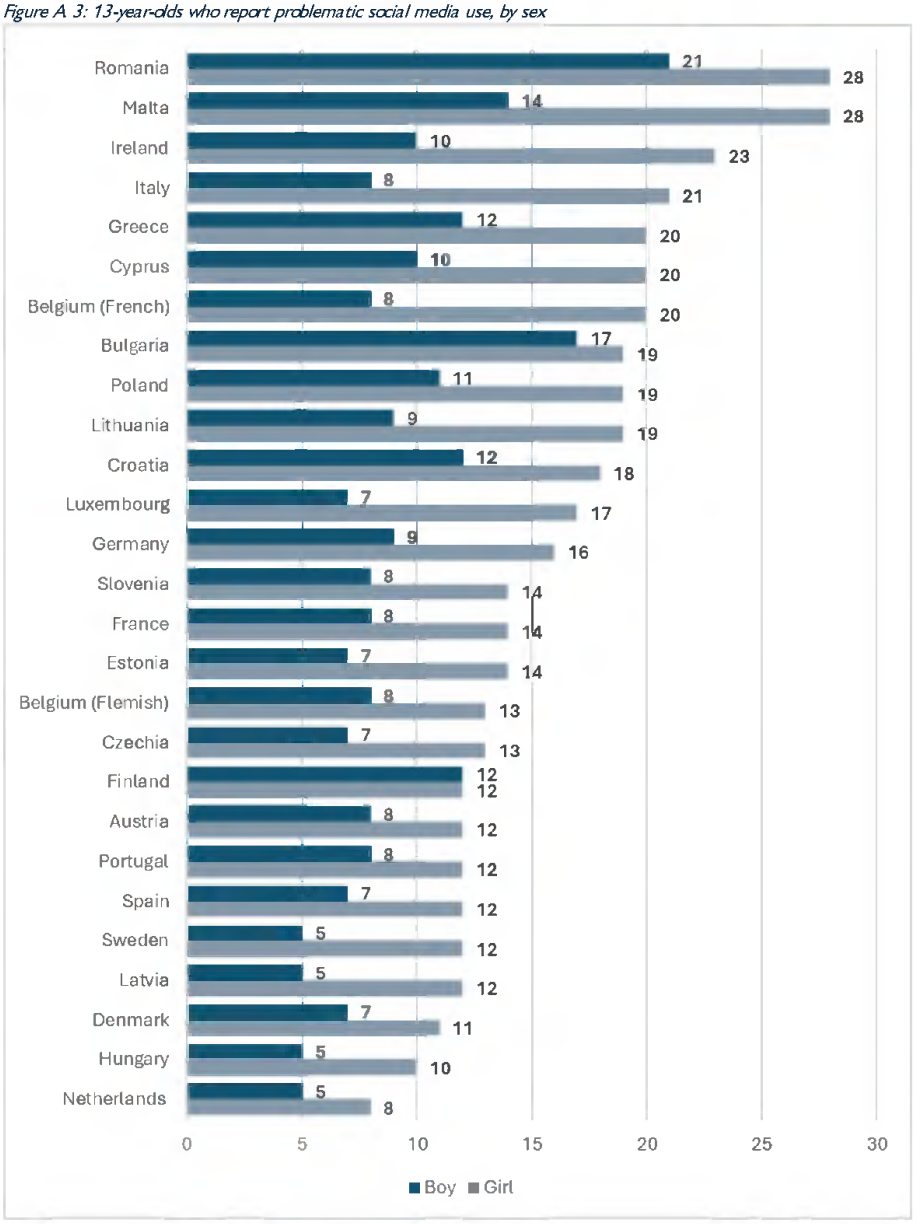
Figure A 2: 15-year-olds who have been cyberbullied at least once or twice in the past couple of months, by sex



Note: Young people were asked how often they had experienced cyberbullying (e.g. anyone sending mean instant messages wall postings or emails or someone posting or sharing photos or videos online without their permission). Response options ranged from I have not been cyberbullied in the past couple of months to several times a week. Findings presented here show the proportions who had experienced cyberbullying at least once or twice a month in the past couple of months.

Source: Health Behaviour in School-aged Children study (2023), Data browser (findings from the 2021/22 international HBSC survey): https://data-browser.hbsc.org

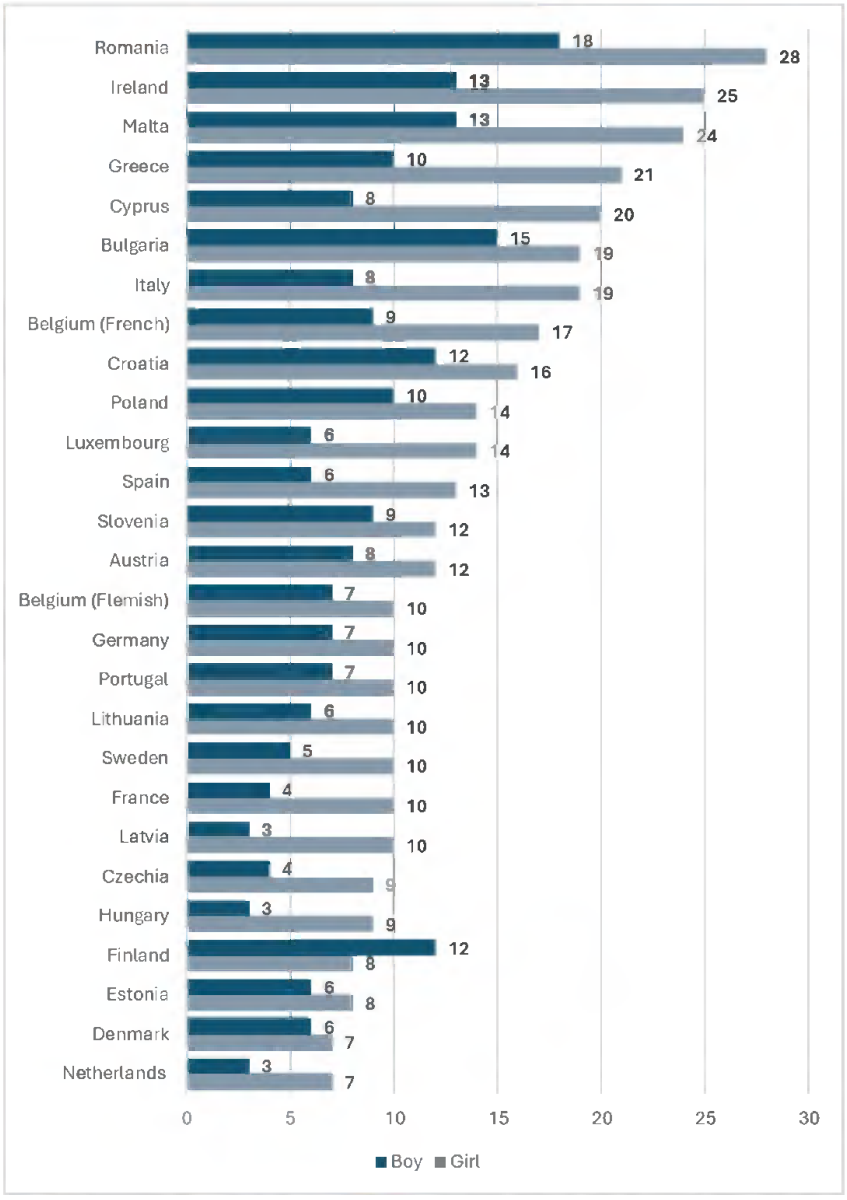
Figure A 3: 13-year-olds who report problematic social media use, by sex



Note: *Young people were asked to report about symptoms of problematic (addictive-like) social media use using the Social Media Disorder Scale a nine-item measure to which respondents answered with yes or no. Findings presented here show the proportions who answered yes to six or more symptoms and were therefore categorised as problematic social media users.*

Source: Health Behaviour in School-aged Children study (2023), Data browser (findings from the 2021/22 international HBSC survey): https://data-browser.hbsc.org

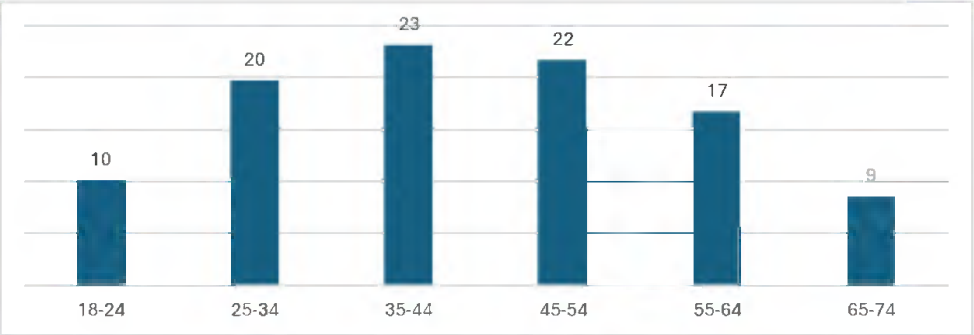
Figure A 4: 15-year-olds who report problematic social media use, by sex



Note: *Young people were asked to report about symptoms of problematic (addictive-like) social media use using the Social Media Disorder Scale a nine-item measure to which respondents answered with yes or no. Findings presented here show the proportions who answered yes to six or more symptoms and were therefore categorised as problematic social media users.*

Source: Health Behaviour in School-aged Children study (2023), Data browser (findings from the 2021/22 international HBSC survey): https://data-browser.hbsc.org

Figure A. 5: People experiencing controlling behaviour from partners who insist on knowing their whereabouts - by age (%)

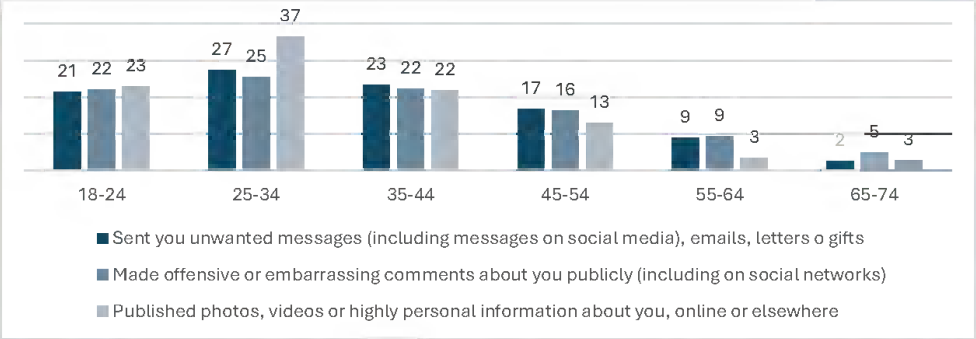


"Note: Respondents were asked whether any of their partners, including current and previous partners had ever insisted on knowing where they were in a controlling way or tracking them via GPS, phone, social network, etc."). (survey question F1)

The findings presented here show the proportion of respondents who reported such experiences, broken down by age, based on the population estimate derived from the sample and appropriately weighted. The target population of the EU-GBV survey is defined as individuals aged 18u74 living in private households, with a focus on women."

Source: Authors elaboration from EU-GBV survey (wave 2021).

Figure A 6: Women having experienced cyber violence by type of violence and age group (%, 18-74, EU, 2021)

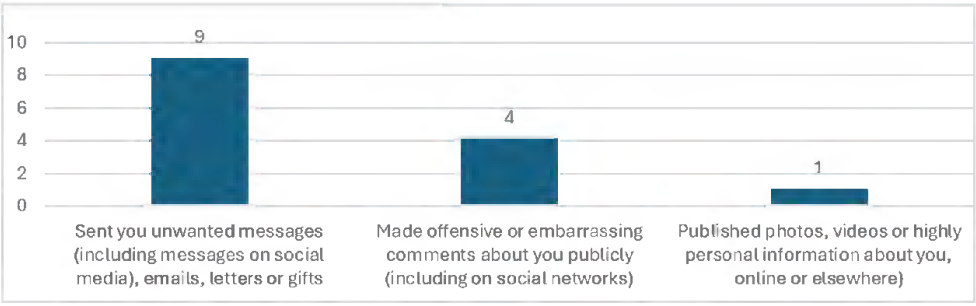


"Note: Respondents were asked whether, during their lifetime, the same person had repeatedly (more than once) carried out one or more of the following actions in a way that caused fear, alarm, or distress. The items considered for this calculation are related to issues linked (though not limited) to typologies of cyberviolence, specifically: , Sent you unwanted messages (including messages on social media), emails, letters or gifts"; , Made offensive or embarrassing comments about you publicly (including on social networks)"; , Published photos, videos or highly personal information about you, online or elsewhere." (survey question N1, survey variables: ST_GIFTS, ST_COMMENT, ST_PUBLISH)

The findings presented here show the proportion of respondents who reported such experiences, broken down by age, based on the population estimate derived from the sample and appropriately weighted. The target population of the EU-GBV survey is defined as individuals aged 18u74 living in private households, with a focus on women."

Source: Authors elaboration from EU-GBV survey (wave 2021).

Figure A 7: Type of violence experienced by respondents (%)

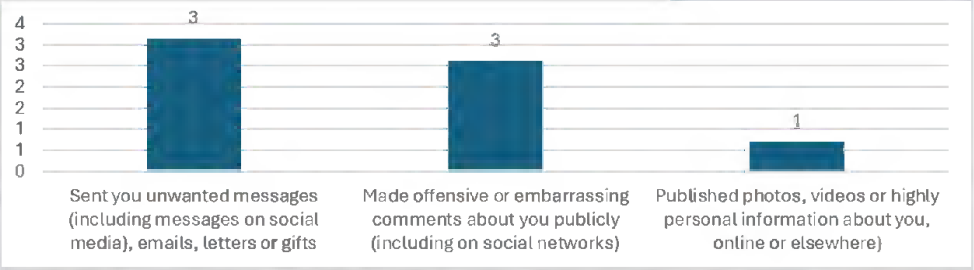


"Note: Respondents were asked whether, during their lifetime, the same person had repeatedly (more than once) carried out one or more of the following actions in a way that caused fear, alarm, or distress. The items considered for this calculation are related to issues linked (though not limited) to typologies of cyberviolence, specifically: , Sent you unwanted messages (including messages on social media), emails, letters or gifts"; , Made offensive or embarrassing comments about you publicly (including on social networks)"; , Published photos, videos or highly personal information about you, online or elsewhere." (survey question N1, survey variables: ST_GIFTS, ST_COMMENT, ST_PUBLISH)

The findings presented here show the proportion of respondents who reported such experiences, based on the population estimate derived from the sample and appropriately weighted. The target population of the EU-GBV survey is defined as individuals aged 18u74 living in private households, with a focus on women."

Source: Authors elaboration from EU-GBV survey (wave 2021).

Figure A 8: Occurrence of the experiences of the type of violence before 15 years-old (%)



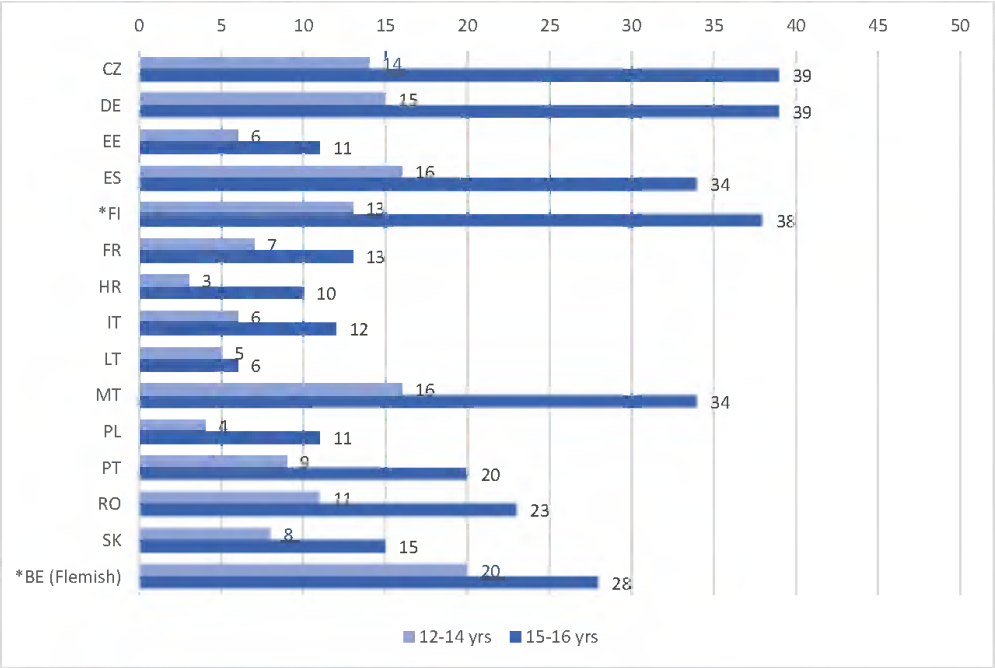
"Note: Respondents were asked whether the episode they experienced happened before the age of 15.

The findings reported here refer to those respondents who - among those who stated in Question N1 that they had experienced an episode linked to the typologies of cyberviolence - answered that among all the situations they had indicated in N1, they had experienced ""all of them"" (survey question N6).

The findings presented are based on the population estimate derived from the sample and appropriately weighted. The target population of the EU-GBV survey is defined as individuals aged 18u74 living in private households, with a focus on women."

Source: Authors elaboration from EU-GBV survey (wave 2021).

Figure A 9: Children having received unwanted sexual requests on line, by age group and country (%, 12-18, EU, 2020)

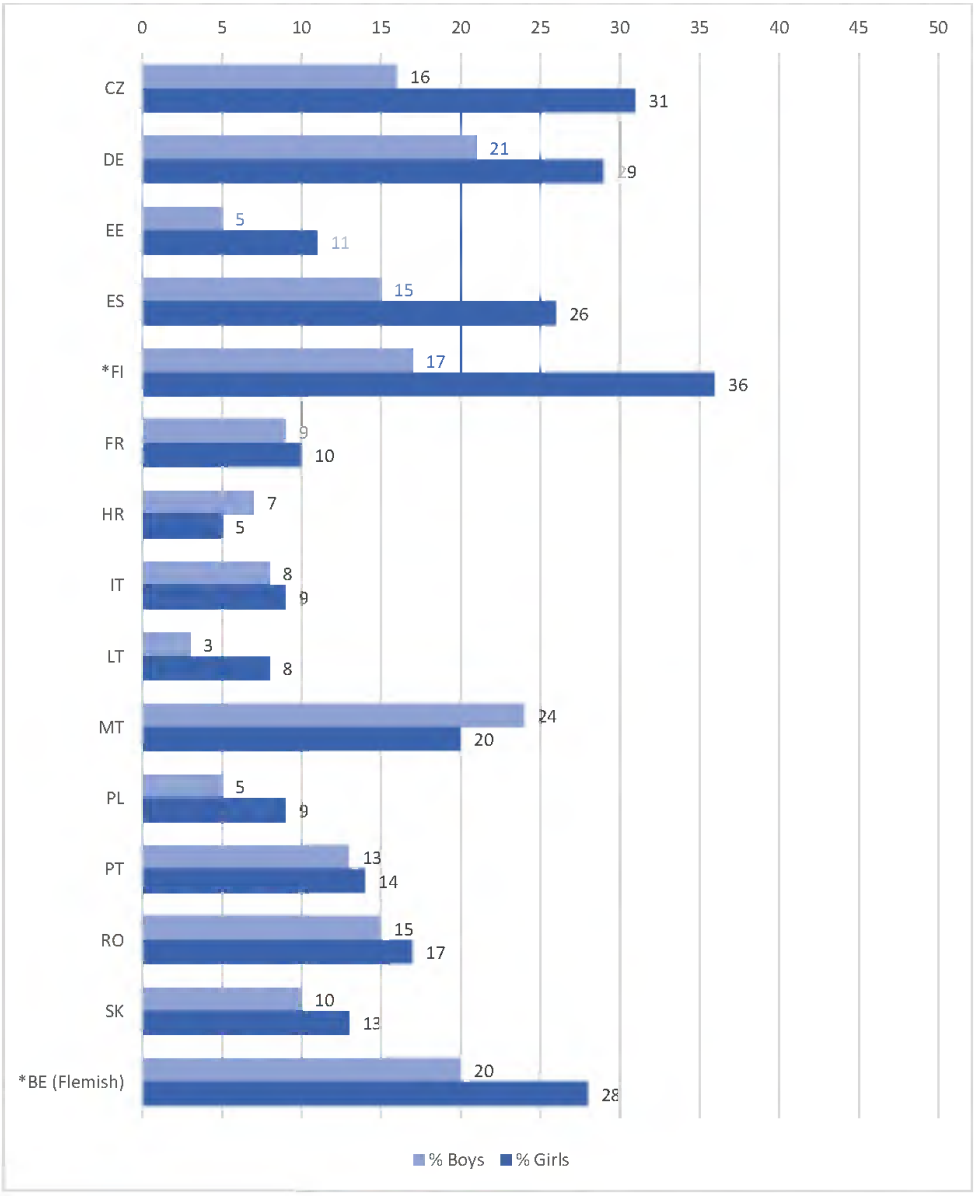


**FI/BE (Flemish): data not weighted*

QF47: In the PAST YEAR, how often, if ever, have you been asked by someone on the internet for sexual information (words, pictures or videos) about yourself when you did not want to answer such questions? Percentage of children who answered a few times, at least monthly or daily or almost daily.

Source: EU Kids Online project, 2020

Figure A 10: Children having received unwanted sexual requests on line, by sex and country (%, EU, 2020)



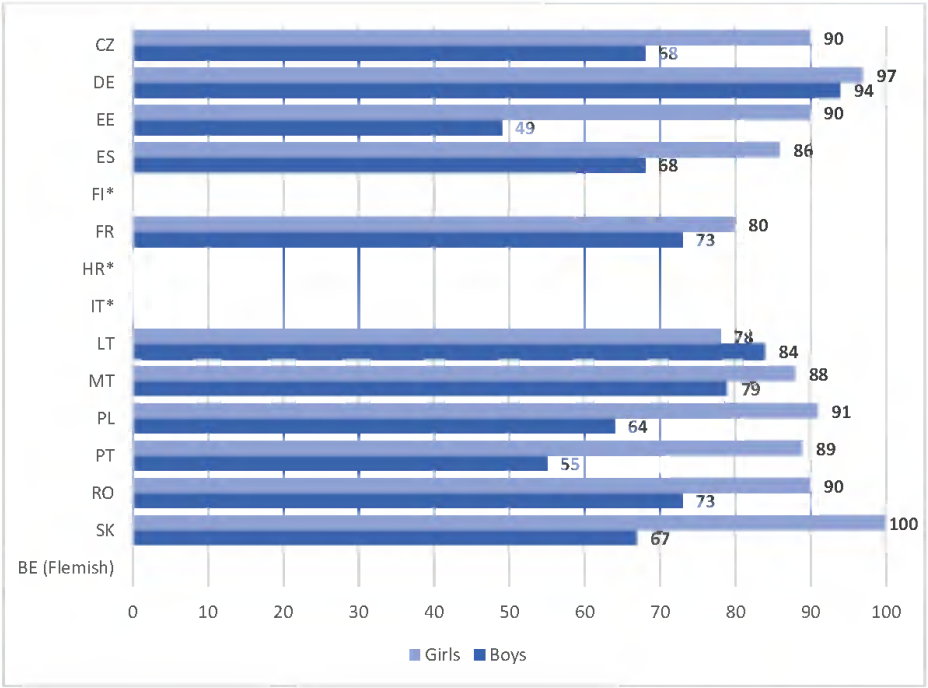
**FI/BE (Flemish): data not weighted*

QF47: In the PAST YEAR, how often, if ever, have you been asked by someone on the internet for sexual information (words, pictures or videos) about yourself when you did not want to answer such questions? Percentage of children who answered a few times, at least monthly or daily or almost daily

Base: All children 9–16 who use the internet

Source: EU Kids Online project, 2020

Figure A 11: Harm from online victimisation (at least a bit upset), by sex



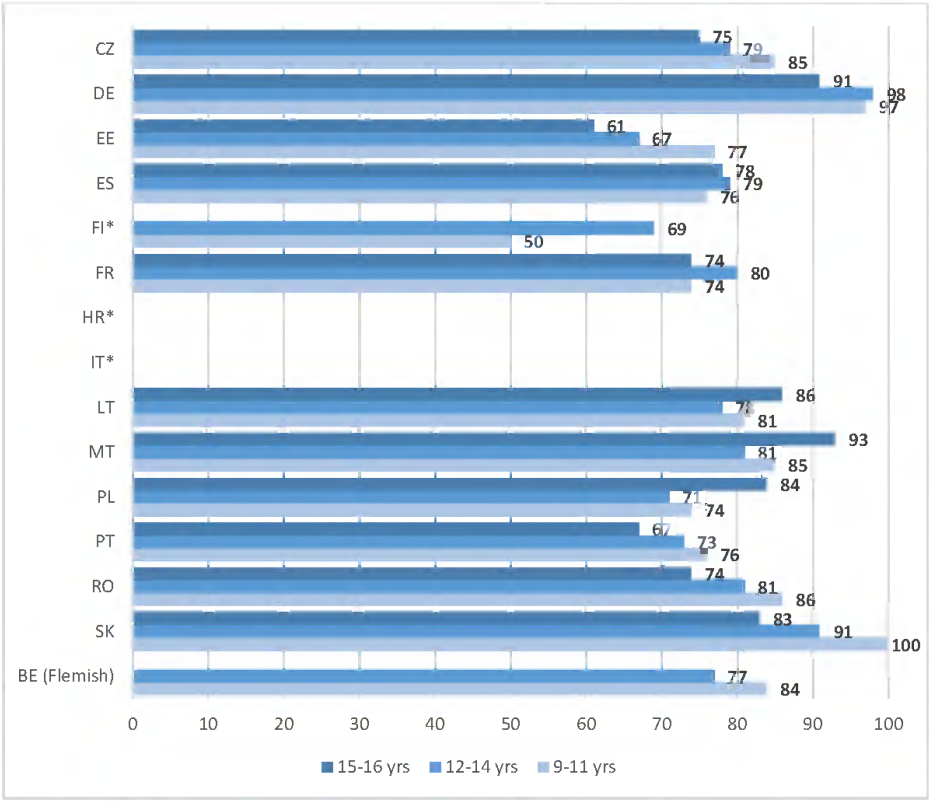
*Note: *FI/BE (Flemish): Full age range not available. HR/IT: Question not asked.*

QF24 Thinking of the LAST TIME someone treated you in a hurtful or nasty way ONLINE, how did you feel? Percentage of children who answered I was a little upset, I was fairly upset, or I was very upset.

Base: All children 9–16 who use the internet and who reported being victimised online at least a few times.

Source: EU Kids Online 2020: Survey results from 19 countries. Available at https://www.eukidsonline.ch/files/Eu-kids-online-2020-international-report.pdf

Figure A 12: Harm from online victimisation (at least a bit upset), by age



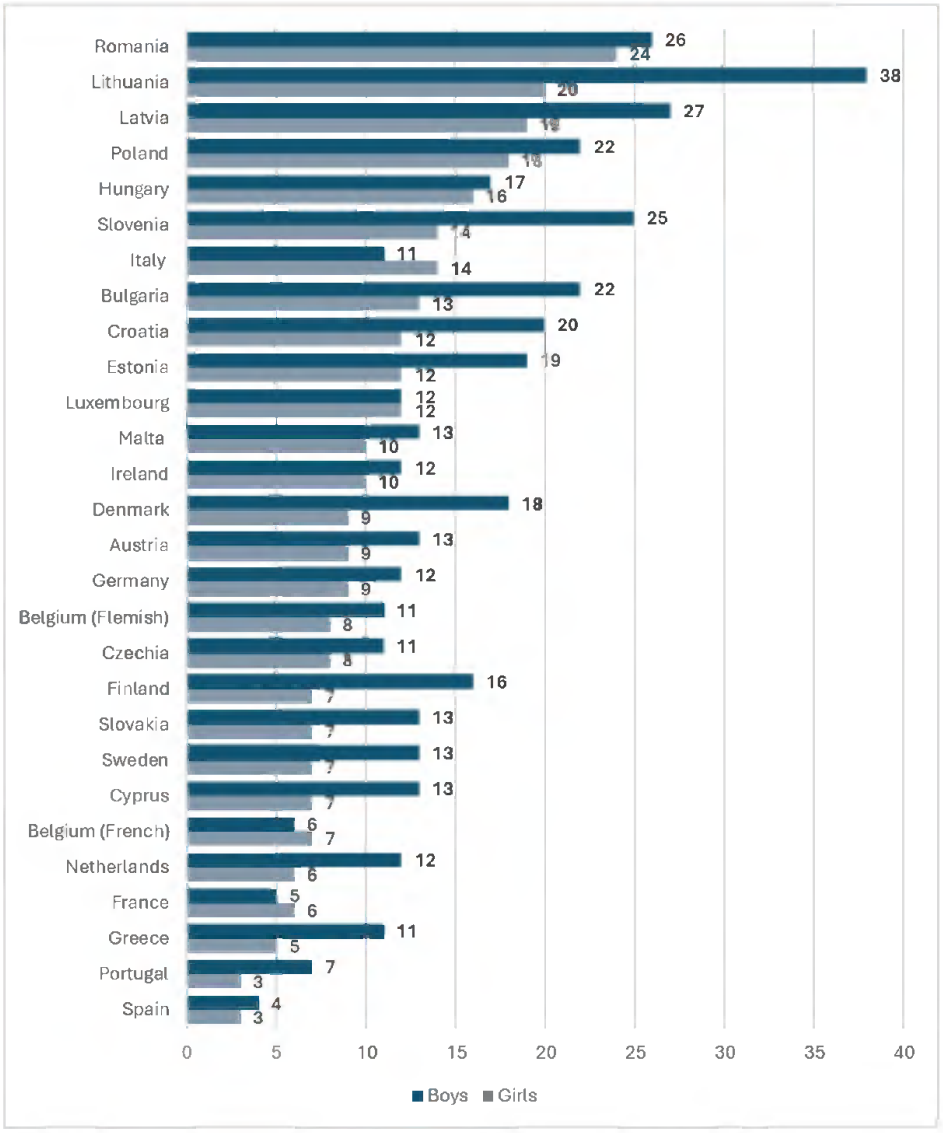
*Note: *FI/BE (Flemish): Full age range not available. HR/IT: Question not asked.*

QF24 Thinking of the LAST TIME someone treated you in a hurtful or nasty way ONLINE, how did you feel? Percentage of children who answered I was a little upset, I was fairly upset, or I was very upset.

Base: All children 9–16 who use the internet and who reported being victimised online at least a few times.

Source: EU Kids Online 2020: Survey results from 19 countries. Available at https://www.eukidsonline.ch/files/Eu-kids-online-2020-international-report.pdf

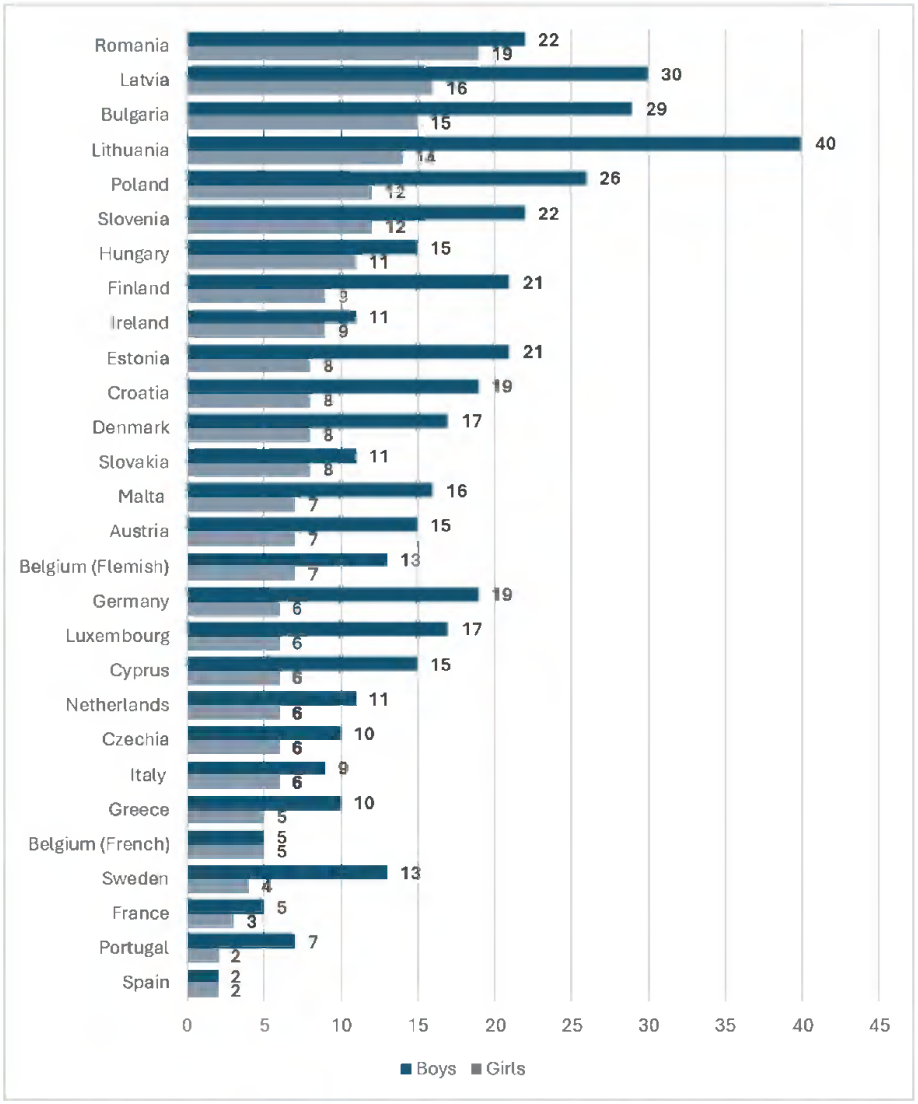
Figure A 13: 13-years old who have cyberbullied others at least once or twice in the past couple of months, by sex



Young people were asked whether they had taken part in cyberbullying (such as sending mean instant messages, wall posting or emails, or posting or sharing photos or videos online without permission). Response options ranged from I have not cyberbullied another person in the past couple of months to several times a week. Findings presented here show the proportions who had cyberbullied others at least one or twice in the past couple of months.

Source: Health Behaviour in School-aged Children study (2023), Data browser (findings from the 2021/22 international HBSC survey): https://data-browser.hbsc.org.

Figure A 14: 15-years old who have cyberbullied others at least once or twice in the past couple of months, by sex



Young people were asked whether they had taken part in cyberbullying (such as sending mean instant messages, wall posting or emails, or posting or sharing photos or videos online without permission). Response options ranged from I have not cyberbullied another person in the past couple of months to several times a week. Findings presented here show the proportions who had cyberbullied others at least one or twice in the past couple of months.

Source: Health Behaviour in School-aged Children study (2023), Data browser (findings from the 2021/22 international HBSC survey): https://data-browser.hbsc.org.

Tables

Table A. 1: Examples of international policy and legal documents addressing cyber violence

Instrument	Year / Body	Scope and main provisions	Cyber violence dimension	Relevance for EU action
UN Women and WHO research paper on Technology-Facilitated Violence against Women (TF VAW)	2023, UN Women and WHO	Highlights gaps in data collection; offers methodologies for better evidence.	Calls for inclusion of diverse experiences in policymaking.	Supports EU's emphasis on data-driven policymaking and intersectional approaches.
UN General Assembly Resolution on violence against women in digital contexts	2021, UN	Calls for international cooperation, platform accountability, and education to empower girls online.	Urges governments to criminalise digital abuse; calls on tech companies for stronger moderation, transparency, and safety tools.	Sets global political standards that inform EU debates and platform regulation.
GREVIO General Recommendation No. 1 on the digital dimension of violence against women	2021, Council of Europe	Guidance on implementation of Istanbul Convention in the digital context.	Emphasises national action plans, digital literacy, and training of law enforcement.	Informs EU recommendations on training, prevention, and digital literacy.
Report of the UN Special Rapporteur on Violence against Women: "Online violence against women and girls from a human rights perspective"	2018, UN	Identifies forms such as cyberstalking, harassment, and non-consensual image sharing; recommends legal reform and systemic change.	Strong focus on victim-centred remedies and education for digital literacy.	Provides human rights framing used in EU Parliament debates and documents.
Convention on preventing and combating violence against women and domestic violence (Istanbul Convention)	2011, Council of Europe	Comprehensive treaty against VAW; requires states to criminalise multiple forms of abuse.	Explicitly includes online abuse (cyberstalking, harassment, non-consensual images).	Basis for EU calls on MS to ratify and implement; aligned with Directive 2024/1385.
Lanzarote Convention on the Protection of Children against	2007, Council of Europe	Protects children from sexual exploitation and abuse.	Includes digital exploitation; Lanzarote Committee guidelines (2017, 2022) stress educating children about digital	Reinforces EU child protection strategies (e.g. Regulation 2021/1232; BIK Strategy).

Sexual Exploitation and Sexual Abuse			safety, promoting age-appropriate content moderation, platform accountability, and cross-sector collaboration among governments, tech companies, NGOs and law enforcement.	
Budapest Convention on Cybercrime and Second Additional Protocol	2001 / 2022, Council of Europe	First binding international treaty on cybercrime; establishes cross-border cooperation and platform accountability.	Covers cyberstalking, grooming, non-consensual images, online exploitation.	Provides legal and operational tools for EU MS in prosecuting cross-border cybercrime.

Source: Author's elaboration

Table A. 2: Examples of EU regulatory developments on gender-based (cyber) violence

	Instrument	Year	Scope and main provisions	Cyber violence dimension	Relevance / Added value
Strengthening legal protections amid emerging challenges	**EU VAW/DV Directive**	2024	Significant legislative commitment to combating CVAWG, as it obliges Member States to act against specific forms of cyber violence crimes.	Provides common definitions for the four main forms of cyber violence. Sets minimum standards for criminalisation and mandates data collection.	Addresses the long-standing issues of diverse and multiple definitions and fragmented approach to criminalisation. Sets up a framework for harmonised data collection likely to improve research and monitoring.
	EU Artificial Intelligence Act (Regulation 2024/1689)	2024	World's first AI law; establishes obligations for high-risk AI and content transparency.	Requires labelling of AI-generated deepfake content.	Direct response to deepnudes/ non-consensual synthetic intimate imagery ; strengthens transparency and accountability.
	Digital Services Act (DSA)	2022	Imposes strict content moderation rules for large online platforms.	Requires proactive moderation of illegal and harmful content, including child sexual abuse material and non-consensual intimate images.	Key enforcement tool for platform accountability. Directive 2024/1385 aligns with DSA's enforcement mechanisms.
	Audiovisual Media Services	2018	Regulates media services across Member States.	Includes provisions against online hate	Extends protection to online platforms; intersectional approach to vulnerable groups.

	Instrument	Year	Scope and main provisions	Cyber violence dimension	Relevance / Added value
	Directive (2018/1808)			speech and harmful content.	
	General Data Protection Regulation (GDPR)	2018	Strengthens rights over personal data; establishes safeguards against misuse.	Enables removal of harmful or non-consensual personal content online.	Provides privacy-based protection frequently used by victims of cyber violence.
Expanding support systems for victims	**Victims' Rights Directive (2012/29/EU, revision proposed in 2023)**	2012 / revision ongoing	Establishes minimum standards for victims' rights and support.	Provides access to counselling, reporting, legal aid; proposals include stronger digital protections for vulnerable groups.	Cornerstone of EU victim-centred approach. Aligned with Directive 2024/1385, that enhances victim support by introducing anonymous online reporting mechanisms, specialised counselling and mental health services, and prevention initiatives (e.g., Article 34.5 of the Directive supporting preventive measures for men).
Monitoring and evaluation through collaboration	**EU Code of Conduct on Countering Illegal Hate Speech Online**	2016 (integrated into DSA in 2025)	Collaboration with major platforms to remove hate speech.	Tackles online hate speech; now reinforced via DSA provisions.	Instrument for public–private cooperation; ensures quicker content removal and accountability online.
Measures to protect children and address	**Regulation (EU) 2021/1232**	2021	Allows detection and removal of child sexual abuse material while ensuring compliance with EU privacy and data	Protects children from online sexual exploitation, including young girls.	Strengthens compliance with privacy standards while combating child sexual abuse material.

	Instrument	Year	Scope and main provisions	Cyber violence dimension	Relevance / Added value
			protection safeguards.		
	Better Internet for Kids Strategy	2022	It promotes digital literacy and online safety across EU Member States.	It addresses cyber violence explicitly via cyberbullying, harmful content, harassment, exposure to sexual abuse content, violent content, self-harm risks etc. Also aims to prevent and respond to harmful conduct among minors online.	Provides a holistic, child-centred framework that links legal/regulatory measures (like DSA) with awareness, education, participation also of children.
	EU Strategies: Gender Equality Strategy 2020–2025; Victims' Rights Strategy 2020–2025; Strategy for a more effective fight against	2020–25	Policy roadmaps for equality, victim protection, and child safety.	Emphasise online gender-based violence prevention, digital literacy, platform accountability, and child protection.	Provide significant guidance on gender-based violence aligning with binding directives.

	Instrument	Year	Scope and main provisions	Cyber violence dimension	Relevance / Added value
	child sexual abuse 2020–2025				

Source: Author's elaboration

Table A. 3: Examples of specific case law related to cyber violence

Type of measure	Country	Name of the measure / year	Description
Case Law	Italy	***Supreme Court Judgment No. 3989/2019*** [63]	In this case, the defendant was convicted of stalking through WhatsApp messages. The individual argued that private messaging between two users should not be considered an electronic means under the law. However, the Italian Supreme Court rejected this argument, affirming that communication via WhatsApp constitutes the use of electronic or telematic means, thereby aggravating the crime of stalking. The Court imposed a six-month prison sentence, emphasising that such messaging platforms fall within the purview of Article 612-bis.
		Supreme Court Judgment No. 33230/2024 [64]	This ruling addressed the distinction between stalking (Article 612-bis) and the unlawful dissemination of sexually explicit images (Article 612-ter, known as 'revenge porn'). The defendant was convicted of both offenses after sending offensive messages and distributing intimate images of his ex-partner via electronic means. The Supreme Court highlighted that the unauthorised sharing of explicit images constitutes a separate offense from stalking, underscoring the legal system's recognition of various ICT-related behaviours as criminal acts.
	Romania	***Supreme Court Judgment No. 56867/15 (Buturugă v. Romania)*** ([65])	In this case, the HUDOC found that Romanian authorities failed to properly investigate both domestic violence and cyberbullying allegations. The applicant reported her former husband's violent behaviour and claimed he had accessed her private electronic accounts without consent. However, the courts dismissed her complaints, arguing that online privacy violations were unrelated to the case. The Court ruled that cyber violations, including unauthorised access to electronic correspondence, are a form of domestic violence and require thorough examination. Romania was found to have violated Articles 3 and 8 of the Convention, and the applicant was awarded EUR 10,000 in non-pecuniary damages.
		Supreme Court Judgment No. 28935/21 (M.Ş.D. v. Romania) ([66])	The case involves the national authorities' handling of the applicant's complaint about alleged online harassment by her former partner, reportedly motivated by revenge, which included the non-consensual public sharing of her intimate photographs. The ECHR determined that Romania infringed upon a woman's right to privacy and family life by not providing protection against cyber violence.

[63] Stalking by WhatsApp - VGS
[64] Supreme Court Ruling: The Boundary Between Stalking and Revenge Porn - Bianucci
[65] Case of Buturugă v. Romania - European Court of Human Rights
[66] Case of M.Ş.D. v. Romania - European Court of Human Rights

Source: Author's elaboration

Table A. 4: Experiences of cyber violence among young people, by age and sex (%)

	Offensive name-calling	Spreading of false rumours about them	Receiving explicit images they didn't ask for	Constantly being asked where they are, what they're doing, or who they're with by someone other than a parent	Physical threats	Having explicit images of them shared without their consent	Any cyberbullying
Boys	31	16	15	13	10	5	43
Girls	32	29	19	17	10	8	49
White	35	24	16	14	10	6	48
Black	29	17	21	9	11	10	40
Hispanic	29	21	19	21	10	7	47
Ages 13-14	29	20	11	12	10	4	42
15-17	34	24	22	17	10	8	49
Boys 13-14	31	15	11	12	10	3	41
Boys 15-17	32	16	18	13	10	7	44
Girls 13-14	25	24	10	12	9	5	41
Girls 15-17	36	33	25	20	10	9	54

Note: White and Black teens include those who report being only one race and are not Hispanic. Hispanic teens are of any race. Those who did not give an answer are not shown.

They were asked: Thinking about your experiences online or on your cellphone, which of the following, if any, has ever happened to you personally?

Source: survey conducted April 14-May 4, 2022. "Teens and cyberbullying 2022"

Table A. 5: Types of cyber violence experienced or witnessed by female focus group participants by country and age (13-18, March-June 2025)

Type of Cyber violence	Description	Relevance to forms of cyber violence covered by Directive (EU) 2024/1385	Example Quotes
(Sexual) Cyber violenceharassment	Includes unsolicited sexual messages or images, grooming, coercion for nudes, revenge porn, deepfakes, and sexual threats.	Cyber harassment (including cyber bullying)	"And there's this app called Snapchat. And on this app this particular friend of mine was totally adding everyone who invited her to it. And it was just like, you'd go into these messages and every message was just a naked penis." (Poland, 13-15)
			"I was on this Omegle already with my friends on a sleepover [sleepover at a friend's house]. This is typical on sleepovers. I connected with a guy like that. I'm like "hey", "where are you from", a conversation, and suddenly I'm „wait, what are you doing?", I'm like uuuuuuuuuu, he put out his cock. It's all the time! Hello, hello, skip, skip, skip! And then 3 some skips later it was the same thing." (Poland 13-15)
			"Not only was he 19, but it wasn't just one person, it was three people sharing one account and writing to underage kids on Discord as a character they had made up. And they were also scamming these kids with 'nudes' and 'softs' and stuff like that." (Poland, 13-15)
			"TikTok in some countries now has the possibility that you can just post pictures in the comments section and some people literally post porn in there, gifs of some kind, something like that. It can be a photo, it can be a gif of a few seconds and very often it can be porn. It can even be anything, maybe a joke, something funny, maybe you'll get comments like this, such a big dick and it's even moving." (Poland, 13-15)
			"For example, a female friend writes back, 'I'm sorry, I'm underage, please don't write to me', and a man of 50+ writes back, 'it's okay, I don't mind'. So, I think in that respect it kills me. But that you write back "I'm underage" and the guy replies "cool, it doesn't bother me". Like you're apologising for something." (Poland, 16-18)
			"… there was this person who, from his profile, seemed to be an older man who sent messages because this girl had an Instagram profile and he kept sending her various provocative messages, asking her to send him photos of herself in her underwear or even without, perhaps in certain

Type of Cyber violence	Description	Relevance to forms of cyber violence covered by Directive (EU) 2024/1385	Example Quotes
			positions, not the most appropriate. And every time she blocked him, he created other profiles and continued to write to her, so he didn't accept rejection."(Italy, 13-15)
			"Yes, or an account called "Horny in [city]" added you. That's not unusual either. Or "sending nudes" not unusual either. Horny guy from [city], a lot of them. I can even go to my snap now and there are several of them where they're just like "horny, looking for a pretty girl". (Sweden, 13-15)
			"I was in a group with a very immature boy. He sent me a private message once and then it continued... At least every three months, let's say... and he would write to me, let's say—how can I put it—if I wanted to send him a message, if I wanted him to send me a message, if I wanted to have sex, this and that." (Cyprus, 16-18)
Cyberstalking	Persistent unwanted contact, tracking via fake accounts, emotional manipulation (e.g., suicide threats), and monitoring in relationships.	Cyberstalking	"It feels like the first thing a guy asks for when you add him on Snap is about you, but then always a picture. It's always pictures..." (Sweden, 16-18)
			"One of my classmates told us about an incident involving an older man who kept writing to her on Instagram asking her to send him certain photos… And every time she blocked him, he created other profiles and continued to write to her, so he didn't accept rejection". (Italy, 13-15)
			"This guy would do anything to get her back, stalking her, sending her messages, and trying to deprive her of everything... but she was just a girl, I don't think she was even fifteen". (Italy, 16-18)
			"After a while he became a bit possessive and when she broke up with him, he tried to track him down through other accounts and through his friends, even resorting to blackmail, saying he would kill himself or stuff like that." (Italy, 16-18)
			"But also like a girl in my class … a guy in my class is obsessed with her. And we've tried for so long to get teachers and stuff to understand it, but he still sends pictures of when he's held knives to his arms and said, "if you don't stay with me I'll kill myself". (Sweden, 13-15)

Type of Cyber violence	Description	Relevance to forms of cyber violence covered by Directive (EU) 2024/1385	Example Quotes
			"It was some guy who wrote something, and she replied… then he started getting a little creepy. She blocked him, but he kept opening new accounts and writing to her. No matter how much she blocked him, he kept going—and she couldn't know that." (Sweden, 16-18)
Cyber harassment (including cyber bullying)	Hate messages, targeted group chats, exclusion, rumour spreading, and mocking, verbal attacks, humiliation, spreading false stories, and coordinated social shaming that impact mental well-being.	Cyber harassment; Cyber incitement to hatred or violence	"They were online friends. And after a few months, we said, since we're so close, let's show each other our faces. Okay, we showed our faces, and because I was 12 at the time and a bit chubby, they started teasing me and kicked me out of the group." (Cyprus, 16-18)
			"I think we've all noticed, either on TikTok or Instagram, a girl who posted photos and now there are messages you can write to someone when they post a story, which are anonymous, and the things people write to her in those messages are very nasty and have very disgusting content". (Cyprus, 16-18)
			"He started spreading rumours about me, as if to make me pay, and we got to the point where I had the whole class against me. Since my school was small, the rumours spread quickly to the other sections and various classes, and I couldn't take it…spending eight hours at school with everyone staring at you and whispering jokes behind your back." (Italy, 13-15)
			"Some people from my old school had set up a group on messenger. It was just there to just literally talk down on me and my like 2 friends. It was so very silly because they weren't posting, they were directing some pictures in different accounts on Instagram and then commenting on them to each other. Or there was also the fact that they started generating AI stories." (Poland, 13-15)
			"So yes, you've noticed from the lower years that it's mainly this sending around naked pictures and starting rumours and stuff. There were definitely one or two cases in the lower years. I think everyone realised that too. And that's definitely also represented here at our school." (Germany, 16-18)

Type of Cyber violence	Description	Relevance to forms of cyber violence covered by Directive (EU) 2024/1385	Example Quotes
			"… I found out from this one girl that they just had a group where they would send each other pictures of me and this friend of us being together in certain places, that we were going to a bubble tea, for example, and there was a picture of us going from behind. Or when we were at school and he was helping me because I didn't understand something in math and we were both bent over the notebook like that. It was also pictures like that that were just everywhere. And it didn't stop, it didn't stop, even when I left school" (Poland, 13-15)
			"They decided that all of a sudden, they would start calling her names on her public account on Instagram. And they'd start writing really mean things about her. And now there are these notes on Instagram." (Poland, 13-15)
			"There are games like Valorant... where there's an option to enter a voice chat. And I can say... there's not a day where it doesn't happen... I'll say 'hello', they hear it's a feminine voice and it just starts—shouting. There's a lot of that 'go to the kitchen' chatter. If I play badly – they say 'I play badly because I'm a woman'. If I play well – they start arguing even more." (Poland, 13-15)
Image-based cyber violence	Secretly taking or manipulating images/videos, sharing them without consent, or creating sexualised deepfakes.	Non-consensual sharing of intimate images	"Me too, yes, I found out about this, about a person I don't know directly, whom I heard about, and she sent videos to her boyfriend, and these videos went around the whole school and everything." (Italy, 13-15)
			"In my class in the first years of high school, there was a period when parents and teachers had to get involved because some boys photographed the private parts of another classmate and spread the photos around the school and the class, and it came to light". (Italy, 13-15)
			"She didn't want to date him, be in a relationship and he literally made a deepfake of her, and he started just sending it around school. Then he hacked her account and her sister's Facebook account, and he started sending just these deepfakes from this friend of mine's account to literally all the contacts that they both had." (Poland, 13-15)

Type of Cyber violence	Description	Relevance to forms of cyber violence covered by Directive (EU) 2024/1385	Example Quotes
			"I was with a guy who I later found out had taken a picture of me when we had sex, it hasn't been shared but I'm still like this, he can keep it, he can keep it. It's unsafe to know that it's there, because even if he deleted it, he could still have it on his phone." (Sweden, 13-15)
			"Then he probably started sending my videos, our videos, we made videos. Sending our videos and my pictures and then... And I know it's kind of wrong, but I just find it sad because I just trusted him with my body like that. And then he sends it to everyone" (Germany, 13-15)

Table A 6: Children having been cyberbullied at least once or twice in the past couple of months by country, sex and family affluence (%, 11-18, EU, 2021/2022)

		Low FAS	High FAS
Lithuania	*Girls*	22	23
	Boys	32	31
Latvia	*Girls*	28	24
	Boys	23	21
Poland	*Girls*	23	20
	Boys	**23**	**29**
Estonia	*Girls*	**27**	**21**
	Boys	**22**	**16**
Ireland	*Girls*	25	21
	Boys	21	15
Sweden	*Girls*	**22**	**29**
	Boys	13	18
Slovenia	*Girls*	20	18
	Boys	**24**	**19**
Hungary	*Girls*	24	18
	Boys	20	17
Bulgaria	*Girls*	22	16
	Boys	19	23
Romania	*Girls*	21	20
	Boys	18	18
Finland	*Girls*	17	19
	Boys	17	20
Croatia	*Girls*	18	18
	Boys	18	16
Czechia	*Girls*	**19**	**20**
	Boys	**15**	**13**
Denmark	*Girls*	19	20
	Boys	14	12
Cyprus	*Girls*	15	16
	Boys	15	15
Slovakia	*Girls*	**19**	**13**
	Boys	16	14
Luxembourg	*Girls*	19	14
	Boys	12	13
Belgium (Flamish)	*Girls*	**21**	**15**
	Boys	12	10
Malta	*Girls*	16	17
	Boys	13	12
Germany	*Girls*	16	13
	Boys	15	10
Italy	*Girls*	19	15
	Boys	11	8
Austria	*Girls*	16	13
	Boys	13	8
France	*Girls*	15	15
	Boys	**9**	**11**
Belgium (French)	*Girls*	15	11
	Boys	10	7
Greece	*Girls*	11	10
	Boys	10	11
Portugal	*Girls*	10	8
	Boys	9	9

		Low FAS	High FAS
Spain	*Girls*	11	6
	Boys	5	4

FAS: Family Affluence Scale. Note: bold indicates a significant difference in prevalence by family affluence group (at P < 0.05). Low- and high-affluence groups represent the lowest 20% and highest 20% in each country/region.

Young people were asked how if they had experienced cyberbullying (such as anyone sending mean instant messages, wall postings or emails, or someone posting or sharing photos or videos online without their permission). Response options ranged from I have not been cyberbullied in the past couple of months to several times a week. Findings presented here show the proportions who had experienced cyberbullying at least once or twice in the past couple of months.

Source: Health Behaviour in School-aged Children study (2023), Data browser (findings from the 2021/22 international HBSC survey): https://data-browser.hbsc.org.

Table A. 7: Prevalence by family affluence: problematic social media use

		Low FAS	High-FAS
Romania	*Girls*	26	28
	Boys	16	18
Malta	*Girls*	21	25
	Boys	14	16
Ireland	*Girls*	23	17
	Boys	11	13
Italy	*Girls*	**24**	**16**
	Boys	10	10
Bulgaria	*Girls*	19	14
	Boys	12	13
Belgium (French)	*Girls*	10	16
	Boys	10	20
Cyprus	*Girls*	17	17
	Boys	11	9
Greece	*Girls*	17	17
	Boys	7	11
Lithuania	*Girls*	18	14
	Boys	9	12
Croatia	*Girls*	11	14
	Boys	**11**	**16**
Poland	*Girls*	13	14
	Boys	9	9
Luxembourg	*Girls*	17	13
	Boys	7	7
Germany	*Girls*	16	11
	Boys	8	8
France	*Girls*	14	13
	Boys	6	8
Slovenia	*Girls*	12	11
	Boys	9	9
Belgium (Flemish)	*Girls*	**14**	**9**
	Boys	8	9
Austria	*Girls*	**12**	**7**
	Boys	**11**	**9**
Spain	*Girls*	16	11
	Boys	5	6
Portugal	*Girls*	10	10
	Boys	8	8
Estonia	*Girls*	**14**	**9**
	Boys	7	6
Czechia	*Girls*	11	11

		Low FAS	High-FAS
Finland	*Boys*	6	7
	Girls	7	7
Sweden	*Boys*	9	11
	Girls	11	12
Denmark	*Boys*	3	7
	Girls	12	8
Latvia	*Boys*	8	6
	Girls	11	8
Hungary	*Boys*	4	6
	Girls	8	8
	Boys	7	5

FAS: Family Affluence Scale. Note: bold indicates a significant difference in prevalence by family affluence group (at P < 0.05). Low- and high-affluence groups represent the lowest 20% and highest 20% in each country/region. Young people were asked to report about symptoms of problematic (addictive-like) social media use using the Social Media Disorder Scale a nine-item measure to which respondents answered with yes or no. Findings presented here show the proportions who answered yes to six or more symptoms and were therefore categorised as problematic social media users.

Source: Health Behaviour in School-aged Children study (2023), Data browser (findings from the 2021/22 international HBSC survey): https://data-browser.hbsc.org.

Table A. 8: Common types of perpetrators of cyber violence

Type of Perpetrator	Tactic	Means Used
The Troll / The Cyber Sexual Harasser	Attacks women who assert their opinions online	Comments sections, forums, chat rooms
The Creepshotter / The Digital Voyeur	Photographs women and girls without their consent and publishes their photos online	Offline public places, Reddit, dedicated websites, social networks
The Revenge Pornographer / The Digital Rapist	Posts private pictures or videos of a sexual nature to shame and humiliate the victim. Extension of intimate partner violence	Social networks
The Online Groomer / The Child Sexual Abuser	Builds a relationship with a child via the internet to bring them into sexual abuse/sex trafficking	Social networks, forums
The Cyberstalker / The Obsessive Abuser	Spies, fixates on, and compiles information about women online to scare them and blackmail them	Social networks
The Masculinist / The Woman Hater	Negates and perpetuates systemic sexism by "defending men's rights"	Dedicated websites, women's groups' websites, social networks
The Cyberbully / The Humiliator	Repeatedly sends hurtful messages and starts rumors to shame and humiliate	Social networks, communication apps
The Dating Website Manipulator / The Sexual Predator	Seeks power and control over their victim by charming them online and luring them towards a dangerous situation	Dating websites, social networks, chat rooms, communication apps
The Recruiter / The Rape Seller aka The Trafficker	Uses new technologies to lure victims, traffic, and sell them for prostitution	Sales websites, dedicated platforms, social media, communication apps

The Doxxer / The Data Thief and Criminal Shamer	Researches and publishes private information online to publicly expose, out, and shame victims	Victim's social network profiles, Google searches
The Malicious Distributor / The Dangerous Defamatory	Uses new technologies and propaganda tools to promote violence against women or women's rights groups	Social networks
The Hacker / The Invader	Intercepts private information and communication (e.g., webcams)	Can be anywhere

Source: Authors elaboration from European Women's Lobby (EWL) proposed classification

Table A. 9: factors influencing behaviour of young bystanders under 20 years of age in cyber violence

Type	Category	Summary
Contextual	**Friendship**	Friendship influences bystander behaviour; positive relationships with victims encourage help, while strong ties with offenders inhibit intervention.
	Social environment	Social norms and support systems influence behaviour. Positive environments encourage intervention, while norms supporting bullying or rejection discourage it.
	Bystander effect	The likelihood of intervention decreases as the number of bystanders increases (diffusion of responsibility). Perceptions of other bystanders' actions also play a role.
	Incident severity	Severe incidents and visible distress in victims motivate bystander intervention.
	Action of other bystanders	Actions of other bystanders influence behaviour; supporting the bully discourages intervention, while defending the victim encourages support.
	Request for assistance	Direct requests for help motivate intervention, as they highlight the seriousness of the situation.
	Evaluation of the situation	Ignorance of the situation or unclear circumstances hinder intervention, while perceived unfairness motivates it.
	Knowledge of strategies	Awareness of effective intervention strategies and support resources encourages positive actions.
	Virtual environments	Online disinhibition and anonymity can encourage negative behaviour, while public communication channels can reduce it.
	Fear of retaliation	Fear of retaliation can discourage action, though strong friendships with victims can mitigate this fear.
Personal	**Empathy**	High empathy levels, especially cognitive empathy, encourage victim-support behaviours, while low empathy can lead to passive or negative actions.
	Moral disengagement	High moral disengagement leads to negative bystander behaviour, while low disengagement promotes helping actions.

Type	Category	Summary
	Behavioural determinants	Factors like self-efficacy, positive attitudes, and prosocial tendencies facilitate intervention, while impulsivity and social anxiety act as barriers.
	Previous experience	Past victims are more likely to help, while previous bullies are more likely to engage in negative bystander actions.
	Demographic data	In some cases, girls and younger individuals are more likely to intervene.

Source: Authors elaboration from Dominguez-Hernandez et al. conclusions of factors, 2018.


European Institute for
Gender Equality
eige.europa.eu